# ExtremeWare Installation and Release Notes

Software Version 7.3.2b3

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: March 2005
Part Number: 120251-00 Rev 01

Alpine, Altitude, BlackDiamond, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, ServiceWatch, Summit, the Summit7i Logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2004 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

NetWare and Novell are registered trademarks of Novell, Inc. Merit is a registered trademark of Merit Network, Inc. Solaris is a trademark of Sun Microsystems, Inc. F5, BIG/ip, and 3DNS are registered trademarks of F5 Networks, Inc. see/IT is a trademark of F5 Networks, Inc.

All other registered trademarks, trademarks and service marks are property of their respective owners.

Author: Susan Lynott

Editor:

Production: Susan Lynott

Special Thanks: Sridhar

# Contents

## Chapter 1 Overview


**New and Enhanced Features in ExtremeWare 7.3** **15**
- Cable Diagnostics 15
- Port Aggregate Bandwidth Control 15
- Standard Multinetting 16
- PIM Snooping 16
- IP Address Security 16
  - *CPU DoS Protect Enhancements* *16*
  - *SNMP Traps and MIBs for CPU DoS Protect* *16*
- IPDA Subnet Lookup 16
- sFlow 16
- Stand-alone ELRP 17
- RADIUS Server Configuration Enhancements in ExtremeWare 7.3 17
  - *Configuring RADIUS Servers* *17*
  - *Configuring RADIUS Authentication and Accounting Servers* *17*
  - *Showing the Current RADIUS Server Authentication Setting* *17*
  - *Configuring a RADIUS Server for Network Login Users (Wired and Wireless)* *18*
  - *Management Access with RADIUS Enabled* *18*
- Trusted Organizational Unique Identifier 20
  - *Trusted OUI and Trusted MAC CLI Commands* *21*
- Link Aggregation Control Protocol (LACP) 23
- Unified Access Feature Support 24
- New .Bxtr Software Image 24

**Supported Hardware** **24**
- BlackDiamond Component Support 25
- Alpine Component Support 26
- Summit Component Support 27
- GBIC Support 28
  - *Mini-GBIC Support* *28*
- XENPAK Module Support 29

**Channel Mapping** **29**

**Tested Third-Party Products** **35**
Tested NICs 35
*WPA-Compliant Wireless NICs* *37*
Tested RADIUS Servers 38
Tested Third-Party Clients 38
Tested Laptops 38
Tested PDAs 38
Tested Tablets 39
Tested Scanner 39
Tested IP Phones 39
Tested Embedded WNIC Modules 39
Tested Spectralink Supported Handsets 39
Tested Spectralink Gateway 39
Legacy IP Phones 39
Legacy Phones with Dongle 40

## Chapter 2 Upgrading to ExtremeWare 7.3

**Staying Current** **41**

**Upgrading ExtremeWare** **41**
PoE Firmware Upgrade 42
Upgrading Switches to ExtremeWare 7.3 42
*Save the Current Configuration* *43*
*Upgrade the BootROM to Version 8.2* *43*
*Upgrade to ExtremeWare 6.1.9* *43*
*Upgrade to ExtremeWare 6.2.2b56* *44*
*Upgrade to ExtremeWare 7.3* *44*
*Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79* *45*
*Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later* *46*
*Upgrade ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 7.3* *46*
*Upgrading PoE Firmware on an Alpine Switch with a PoE Module* *47*
Upgrading an Alpine 3802 to ExtremeWare 7.3 47

**Downgrading Switches** **48**

## Chapter 3 Supported Limits

**Supported Limits** **49**

## Chapter 4 Clarifications, Known Behaviors, and Resolved Issues

**Clarifications and Known Behaviors** **57**
General 57
*optrambusywait Error Message* *57*
*IP Multicast FDB Entry Incorrect* *57*
*LACP Does Not Detect Link Down* *58*
*Smart Redundancy* *58*
*Changing Auto Negotiation* *58*
*ARP Response from MPLS to MSM* *58*

*HTTPS Access* 58
*Unable to Download Image to a Switch with 500 Configured IP VLANs* 58
*NP API Generates Error Messages When Disabling a Slot Containing an OC3 or OC12 Module* 58
*Cannot Ping localHost Loopback Interface* 59
*Hot-swapping an MSM3 Causes Invalid MAC Address on Backplane EEPROM* 59
*MSM-3 Displays Broken Connection Recovered Message when Hot-swapping and Inserting an MSM64i* 59
*Hot-Swapping an MSM Causes I/O Modules to Reset* 59
*Downloaded Configuration Might Cause Syntax Error With Enable Web Command* 59
*Wireless Error Messages Display During Bootup* 59
*show pim snooping Command Shows an Incomplete List of Packets Snooped* 60
*MSM-Failover Link-Down Not Working on the Remote Side* 60
*ExtremeWare 7.3 introduces the concept of QoS profiles on a VLAN* 60
*Repeatedly Hot-Swapping the MSM Might Cause Loss of Connectivity* 60
*Cannot Save or Download a Configuration If a "ghost" Process is Running in the Background* 60
*Creating an ACL with a Filter-Precedence of 11 or 12 Generates a Conflict Error with cpu-dos-protect* 60
*Hot-Swapping Modules Might Cause Misleading Error Messages* 60
*G12Ti Module Link Detection Fails* 61
*Autonegotiation Between Fiber Optic Ports is not Possible* 61
*show log Command Memory Error* 61
*unconfigure switch all Command Should Not Restore the Downloaded Configuration* 61
*WLANSYST Output of the show log Command is Not Correct* 61
System Related – All Systems 61
*The NVRAM Dirty Bit Being Set from the PoE Code* 61
*PoE Firmware image Download is not Available in Base Image* 61
*Autonegotiation Setting Not Preserved on Added and Deleted Loopback Ports* 61
*Configure Slot for PoE Before Configuring or Downloading PoE Configuration* 62
*The show log Command Truncates Long Commands* 62
*The show log Display Truncates Configuration Parsing* 62
*Do Not Create Single-Character Names* 62
*Smart Redundancy Enabled in Saved Configuration* 62
*Telnet and the show ports Command* 62
*The show configuration Output* 62
*Upgrading to ExtremeWare 7.0 and Bi-Directional Rate Shaping* 62
*Upgrading to ExtremeWare 7.0 and Debug-Trace* 63
*Upgrading to ExtremeWare 7.0 and OSPF* 63
*Blank Space in show port info detail Command Output* 63
*Using an ExtremeWare 7.0 Configuration with an Earlier Image* 63
*Console Response with a Large Number of ARP Entries* 63
*The show log chronological Command* 63
*BOOTP-Dependent Routes in Downloaded Configuration not Created* 63
*The disable learning Command and Flooding* 63
*Port Tag Limitation* 63
*WinSCP2 Not Supported* 64
BlackDiamond 64
*Broadcast or Unknown Unicast Packet Sent to Same Ingress Port* 64
*ExtremeWare 7.0 (and Later) Does Not Support xmodem* 64
*Secondary MSM Access Error* 64
*Loopback Port Must be on Same Module on a BlackDiamond Switch* 64

*Two Trap Messages Sent for Hard Reset/Soft Reset on BlackDiamond 6816* 64
*Targeted LDP Sessions Become Operational When MPLS is Disabled* 65
*BGP Fast Fail-over Does Not Work for Change of IP Address* 65
*CMT Group Will Not Forward Traffic Without a Master Slot* 65
*Connection to G12SXi Might be Lost* 65
*MPLS and ESRP* 65
*EAPS and Hitless Failover* 65
*Cross-Module Trunking and Hitless Failover* 65
*Autonegotiation Off Command Accepted on 10 Gigabit Ethernet Modules* 66
*Memory Corruption with RRO on PATH Message* 66
*No Longer Display Stale TLS NHLFE Entries* 66
*MPLS Module Might Not Be Recognized* 66
*LSP NHLFE Not Updated* 66
*Removing Second MPLS Module Causes Traffic to Stop* 66
*Disabling One MSM Might Cause Loss of Throughput* 66
*Cannot Delete an LSP Previously Referenced by a TLS Tunnel* 67
*EAPS Trap Not Sent if Connection is Through I/O Port* 67
*The card-down Option* 67
*10 Gigabit Ethernet and CMT* 67
*XENPAK with the BlackDiamond 6816* 67
*Cross-Module Trunking Not Supported on MSM64i's* 67
*Cross-Module Trunking Module Support* 67
*Master Slot Must Be Active for CMT* 68
*MSM-3 Log Might Be Out of Chronological Order* 68
*Source Addresses Might Age Out of FDB* 68
*Do Not Use Static FDB Entries with CMT* 68
*Saving Health Check Configuration After Failure Causes Console Crash* 68
*Diagnostics on MSM-3 with Hitless Failover Causes Failover and Spurious Message* 69
*Do Not Configure a Port-Based Backplane Algorithm When CMT is Enabled* 69
*Cross-Module Trunking and ACLs* 69
*4,000 VLANs on a BlackDiamond* 69
*E1 Module and the restart port Command* 69
*PPP Links Through E1 modules* 69
*Slot Failure Messages During a Broadcast Storm* 69
*No Image Information Reported to SNMP with One MSM* 69
*BlackDiamond 6816 MSM C and D Diagnostics Messages not in Syslog* 69
*Disabling CLI Paging from the Slave MSM64i* 70
*The unconfig switch all Command* 70
*BlackDiamond 6816 MIB Value for Input Power Voltage* 70
Alpine 70
*Mirroring Failure on an Alpine 3808 with GM4x Module After a Save and Reboot* 70
*With IE5.0 Vista Page is not Accessible Through HTTPS* 70
*Autonegotiation on VDSL Ports Set Incorrect Speed* 70
*VDSL Ports do not Support Jumbo Frames* 70
*New Accounts with WAN Module Installed are pppuser* 70
*Limited Commands Mode* 70
*VDSL Modules in a Half-Duplex Link* 71
Summit 71
*Spurious Summit48si Power Supply Messages* 71
*Output of the show log Command* 71

*The unconfigure switch all Command Clears the Default VLAN from s0* 71
*Health Check Error Messages* 71
*Summit48i Redundant PHY* 71
*Summit48i Single Fiber Signal Loss* 71
*SNMP Results for Power Sources* 71
*Summit48si MIB value for Input Power Voltage* 72
PoE 72
*PoE Firmware Update Can Occasionally Fail* 72
Command Line Interface (CLI) 72
*IGMP Snooping Not Disabled on MAC VLAN* 72
*Mirroring Cannot be Disabled* 72
*Console Does Not Wait for User Input* 72
*Command Does Not Function* 73
*show fdb vpls Command Does Not Accurately Show the Correct Total of FDB Entries* 73
*clear counters Command Does Not Clear Number Transmitted in a MPLS Health Check* 73
*show fdb port Command Does Not Reflect Correct FDB Data for that Port* 73
*Maximum Number of ESRP Groups Supported in the ESRP MIB is Incorrect* 73
*Not All configure debug-trace Options Are Displayed* 73
*SNMP Trap Commands Not Supported* 73
*The show ports mgmt info Output Missing Flags* 73
*Press [Return] Key Twice With enable temperature-log Command* 74
*User Sessions Cannot Enable CLI Paging* 74
Switching and VLANs 74
*Renew/Refresh Required After Each Logout To Get IP Address* 74
*Packets Sent to VRRP-MAC That Do Not Belong to the VRID of the VLAN are also Being Accepted* 74
*The show iproute Output* 74
*MAC-Based VLAN Configuration Not Saved* 74
*Load Share Group Might Fail Back to Group with Fewer Ports When Using Software Redundant Ports* 74
*Saving ip-mtu Settings* 75
*VLAN priority and STP, EDP* 75
*Default Routes or Static Routes* 75
*Configuring a Protocol Filter with 'ffff'* 75
*Deleting Protocols from a VLAN* 75
*MAC-Based VLANs and DHCP Relay* 75
*VLAN to VLAN Access Profiles* 75
FDB 75
*FDB Entries Disappear Before Aging Timeout* 75
*Cannot Add FDB Entry for Management VLAN* 76
*MAC Security* 76
*FDB Aging Timer* 76
*Configure Less Than 400 Ports in a VLAN* 76
Load Sharing 76
*Removing Modules During CMT Testing Causes Loss of Traffic* 76
*Backplane Algorithm Not Working Properly When Changing the Algorithm from Address-Based to Port-Based* 76
*Autonegotiation* 76
*Round Robin Load Sharing* 76
*Port Based Load Sharing on Summit7i* 77

*Alpine and Cross Module Load Sharing* 77
*Load Sharing and Specific Ports in a Load Share Group* 77
*Disabling Load Sharing if the Master is Down Generates Error* 77
Mirroring 77
*Port Mirroring Does Not Work on Rate Shaping Loopback Port* 77
*Delete Mirroring Filters Before Disabling Mirroring* 77
*Port from Deleted VLAN Mirrors When Added to New VLAN on Alpine Switch* 77
*Do Not Configure Port Mirroring While Port is Down* 77
ELSM 78
*Spurious Error Message with ELSM* 78
Spanning Tree 78
*Adding or Deleting a Port from a VLAN Flushes FDB on All STP Protected VLANs* 78
*show vlan STP Output is not Correct* 78
*STP Topology Change in One STP Domain (S1) Flushes FDB in Other STP Domain (S2)* 78
*STP CPU Utility Usage Increases and Drops Ping Packets* 78
*Disabling ignore-bpdu Adds CPU MAC Entry to FDB* 78
*Enabling STP on MAC-based VLANs Might Cause Connectivity Loss* 78
*Incorrect Log Message* 78
*RSTP Does Not Detect Topology Change* 79
*Disabling STP Might Display Topology Change* 79
*FDB Not Flushed After Link Failure with RSTP* 79
*Do Not Configure All Ports in s0* 79
*Error Messages with Topology Changes* 79
*Large STPD Configuration Download Might Reboot Switch* 79
*A Large STP Configuration with 10 Link Transitions* 79
*Configure Fewer than 4,000 VLANs in an STPD* 79
*Output of show stpName port detail Command in Hex Format* 79
*If You Delete a Port from the STPD, You Cannot Add It Through a VLAN* 80
*The unconfigure stp Command Does Not Clear All Configurations* 80
*Enabling ignore-bpdu or ignore-stp* 80
*Configuring a VLAN from Vista* 80
*STP and VLAN Tagging* 80
*EMISTP and Ingress Rate Shaping* 80
*Upgrading From an ExtremeWare 6.1.9 (or earlier) Configuration* 80
ESRP 80
*ESRP Master Does Not Change to the Neutral State* 80
*The disable slot all Command Generates EDP Errors* 81
*Large Configurations Might Lock Console when Enabling and Disabling s0* 81
*ESRP and Protocol-Based VLANs* 81
*ESRP and Load Sharing* 81
*Hot-Swapping a Module with 5,000 ACLs* 81
*Traffic Convergence Time* 81
*ESRP PDUs on Ports* 81
ELRP 81
*ELRP and Ingress Rate Shaping* 81
VRRP 82
*Proxy ARP Replies on VRRP Enabled VLANs Are Incorrect* 82
*Backup Transition Creates Duplicate Packets* 82

QoS 82
*DiffServ QoS Priorities Apply Per Block* 82
*QoS Profiles Applied to Non-Master Ports in Load Sharing Groups* 82
*QoS Profile Statistics Are Not Shown for Non-master Ports in a Loadshared/CMT Group* 82
*The qosprofile Accepts a Value Greater than 100%* 82
*Re-Ordering Access List Precedence Numbers* 82
*Access List FDB Entries not Cleaned Up* 82
*Access Lists Using the IP Deny Any Rule* 83
*Access Lists and IP Fragmentation* 83
*QoS Configuration Bandwidth Parameters* 83
*Creating Access Lists from Multiple Sessions* 83
*5,120 Access Lists and SNMP* 83
*Monitoring QoS and the show port qos Command* 83
MPLS 83
*Cannot Delete TLS VLAN After Deleting TLS Tunnel When MPLS is Disabled* 83
*IP Interface of Local End-point VLAN for TLS Tunnel or VPLS Can be Modified* 83
*Clear Counters Command Does Not Clear RSVP LSP Count* 84
*Targeted LDP Sessions Become Operational When MPLS is Disabled* 84
*Targeted LDP Sessions do not Come Up When OSPF is Disabled and Router ID is Automatic* 84
Bi-Directional Rate Shaping 84
*Secondary MAC Used for Rate Shaping Not Released* 84
*Aggregate-Bandwidth Granularity Correction* 84
*SecureMac Flags Not Shown* 85
*Locking and Unlocking Learning* 85
*1000Base-T Ports as Loopback Ports* 85
EAPS 85
*Cannot Delete a VLAN from EAPS Domain* 85
*Configuring Cross Module Trunking Causes EAPS Failure* 85
*Shared-Port Link ID Limits* 86
*EAPS Performance Statistics* 86
*ESRP and EAPS Secondary Port* 86
*Incorrect show vlan Output* 86
IP Unicast Routing 87
*Reset the FDB Aging Timer* 87
*No Static ARP Entries* 87
*ARP Entry Age* 87
*Multinetting and the Show VLAN Stats Command* 87
*Multinetting and VRRP* 87
IPv4 Routing 87
*PIM CRP Timer Error* 87
RIP Routing 87
*Access Profile Does Not Block Default Route from Being Advertised, in case of RIP Export Filter* 87
*Problems with Default Route Origination Addition and Purging* 87
*RIPv1 Learned Routes Might Not Be Purged Immediately* 88
*RIPv2 Authentication* 88
*RIP in Conjunction with other Routing Protocols* 88
OSPF 88
*Duplicate IP Addresses Causing OSPF Route Flapping* 88
*OSPF Originate Default Cost Can Be Set Incorrectly* 88

*LSA Batch Interval Not Supported* 88
*Static Route with Switch's Address as Gateway Not Advertised* 88
*AS-external LSAs Might Not Be Regenerated* 88
*Error Message Not Generated* 88
*Disable OSPF Before Adding or Removing External Area Filters* 89
IS-IS 89
*Unicast Packets Considered Broadcast* 89
BGP 89
*improper Handling of EXT Length Bit Flag in BGP AS_PATH Attribute* 89
*A Session Down Due to Max Prefix Limit Will Not Re-establish* 89
*Large Number of Access Profiles and a Peer Reset* 89
*Default Route Might Not Be Deleted* 89
*BGP Aggregation with a Maximum Prefix of 300,000* 89
*Redistributing BGP Routes to OSPF* 89
IP Multicast Routing 90
*System Fails After Receiving PIM Bootstrap Packet* 90
*PIM SM Switch Reboot will not Re-establish the Existing Multicast Traffic Present Before Reboot* 90
*PIM DM Switch Reboot Might Delay Re-establishment of Traffic* 90
*(S,G) Packets are Sent to CPU When Route to Source is Lost in Last Hop Router* 90
*The unconfigure igmp Command Does Not Unconfigure All Parameters* 90
*If PIM-Snooping is Enabled on Current Traffic, All (S,G) Entries Will be Marked as Invalid* 90
*Enable or Disable IGMP Snooping on a Sub-VLAN* 90
*Do Not Disable IGMP Snooping with Static Snooping Entries* 90
*(S,G) Entry Not Created if RP is Rebooted* 90
*Cisco Interoperation* 91
*Traffic Rate Exceeding Last Hop Threshold* 91
Network Login 91
*Multiple Supplicants* 91
*TCP SYN and TCP ACK Not Working Correctly* 91
Security 91
*Enhanced DoS Protection Feature Limitation* 91
Changing VLAN and Wireless Port IP Causes RADIUS Proxy Failure 91
*Cannot Apply a New Port after Creating a Trusted MAC Entry on a VLAN* 91
*Unconfiguring a Slot will not Remove the Ports from Network Login and Network Login Cannot be Disabled* 91
*Proxy ARP Setting Should Take Effect When Network Login is Enabled* 92
*Wireless Clients Forced to Reauthenticate During Roaming* 92
*Enhanced DOS Protect Rate-Limit Configurations Are Lost* 92
*Disable Trusted MAC Globally Will Not Automatically Remove Network Login Ports Added as Tagged Port in other VLANs* 92
*After Network Login Authentication, Cannot Get an iP Address from the DHCP Server* 92
*Wireless Ports Do Not Come Online if VLAN Gets IP Address from BOOTP* 92
*Special Characters Accepted in WEP Plaintext Key* 92
*A New ACL Might Not Block Packets* 93
*Roaming Client MAC Might be Aged Out* 93
*False EAPOL-Flooding Alarm* 93
*EAP-Failure Messages Not Sent When Client is Unauthenticated by an Administrator* 93
*Do Not Upload a Configuration Containing Authenticated Clients* 93
*The show netlogin Output Might Display Wrong Authentication* 94
*ICMP Access Lists and ignore-overlap* 94

*CPU DoS Protect and ACL Precedence* 94
*MSM Failover Clears Logins* 94
*Network Login RADIUS Server Interoperability* 94
*Network Login Supplicant Software Interoperability* 95
*RADIUS and the BlackDiamond* 95
*RADIUS and Telnet* 95
*The show netlogin Command Output* 95
SLB and Flow Redirection 95
*Do Not Use SLB and NAT on the Same Switch* 95
*Enumeration Mode Redirects ICMP Packets* 95
*Cache Servers Set To "Down" Under Sustained High Traffic Loads* 96
*Health Checking Cannot be Disabled* 96
NAT 96
*Do Not Use SLB and NAT on the Same Switch* 96
*NAT Rule Configuration Not Updated* 96
Vista 96
*Failed Vista Login Logged Incorrectly* 96
*No 10 Gigabit Option for Port Speed* 96
*SNMP Community and Trapreceiver Information Not Updated* 96
*Use CLI to Configure SNMPv3* 96
*Incorrect Minimum Limit on OSPF Page* 97
*Cannot Create User Accounts* 97
*Cannot Enable STP* 97
*Alpine 3808 Erroneously Displays Four PSUs* 97
*Cannot Add Trap Receiver or Community String* 97
*Blackhole Flag Missing* 97
*Multicast Address Display* 97
*Configuration Statistics PSU Display* 97
*Vista and RADIUS* 97
*Configuration Options with Large Number of Interfaces* 97
SNMP 98
*Extreme Real Time Statistics Does Not Work When There are 24+ Ports* 98
*Performing an SNMP Mibwalk and Polling qBridgeMIB Might Cause High Utilization* 98
*ESRP SNMP MIB Table Election Algorithms Missing* 98
*The configure snmp community Command Replaced* 98
*Only Warm Start Smart Trap Sent After Power Cycle* 98
*extremeVlanGlobalMappingTable Exists only for Backward Compatibility* 99
*ExtremeEapsTable Not Browsable* 99
*MIB Does Not Differentiate Between 110 and 220 VAC* 99
*The trapDestOwner is Required in the trapDestTable* 99
*Cannot Delete Default Community Strings* 99
*Do Not Configure an SNMPv3 Community String with more than 32 Characters* 99
*Modular Switch get Error* 99
*SNMP and ACLs* 99
*Incrementing the Interface Value* 99
*Trap Receivers as Broadcast Entry* 100
*Bridge MIB Attributes* 100
*SNMP Time-out Setting* 100
*SNMP Access Profile* 100

*SNMP and Auto-negotiation Settings* 100
*SNMP and the FDB MIB* 100
*Extreme Fan Traps* 100
*Extreme Power Supply Traps* 100
Diagnostics and Troubleshooting 101
*FDB-Scan Does Not Upgrade Properly* 101
*OC12 Module Might Report False External Loopback Failure on External Test* 101
*A3ci Running Normal Diagnostics Hangs in the "diag" State* 101
*NP Module Error Messages in the Log After Running Diagnostics* 101
*Errors Not Displayed in show diagnostics Output* 101
*Incorrect show diagnostics Output for BlackDiamond 6816* 101
*Entering q Does Not Quit Diagnostics Display* 101
*Single MSM Not Taken Offline* 101
*Automatic Memory Scanning Can Trigger Incorrect Reboot Loop Detection* 102
*Packet Diagnostics Display Backplane Incorrectly* 102
*Packet Diagnostics Display Wrong Slot Name* 102
*Bus-Stats Error Messages* 102
*Spurious Message When system-down is Configured* 102
*The use configuration Command* 102
*Output of the show diagnostics Command* 102
*Configure Auto-Recovery to online or Alarm-Level to traps* 102
*Error Count Not Accurate* 103
*Configuring Diagnostics Mode Off* 103
*Disable Remote Syslog Before Enabling IPARP Debug-Tracing* 103
Bridging 103
*Extended Diagnostics Does Not Include Backplane Connection* 103
Documentation 103
*enable rip originate-default Command Description is Incorrect* 103
*VRRP and ESRP Can Be Simultaneously Enabled* 103
*Summit48si LED Description Incorrect* 103
*reauth-period Range is Not Correct* 104
*EAPS is now supported with Basic Layer 3 License* 104
*The Auto-Recovery Threshold Applies only to BlackDiamond I/O Modules* 104
*Configure Auto Negotiation to Recognize Single Fiber Failure as Port Failure* 104
UAA 104
*TCP Transmission Causes an SNMP Send Error when the AP Comes Up* 104
*Some IAPP Debug Messages Are Not Logged* 104
*DHCP Port is Disabled When Changing a VLAN Tag* 104
*Port Related Configuration Returns an Error During Configuration Download* 105
*ifSpecific Variable of ifEntry Table Shows Incorrect Characters for Wireless Interfaces* 105

**Issues Resolved in ExtremeWare 7.3.2b3 105**
General 105
BlackDiamond 106
Summit 106
Spanning Tree Protocol 106
Bridging 106
Diagnostics 106
EAPS 106

Mirroring 106
RADIUS 106
Routing 106
SNMP 107

**Issues Resolved in ExtremeWare 7.3.1b3 107**
General 107
EAPS 107
Multicast 107
Network Login 107
Security and Access Policies 108
SNMP 108
VLANs 108

**Issues Resolved in ExtremeWare 7.3.0b49 108**
General 108
Alpine 108
Security and Access Policies 109
UAA 109
QoS 109
PoE 109
SNMP 109
ESRP 109
CLI 109

**Issues Resolved in ExtremeWare 7.3.0b44 110**
General 110
Summit 110
BlackDiamond 110
Alpine 111
Vista 111
SNMP 111
Spanning Tree 111
Security and Access Policies 111
Switching and VLANs 112
Network Login 112
Diagnostics 112
VRRP 112
BlackDiamond 112

# 1 Overview

These Release Notes document ExtremeWare® 7.3.2b3. ExtremeWare 7.3 enables new hardware products and software features.

**NOTE**

*You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2 (or later). To install ExtremeWare 7.3, see "Upgrading ExtremeWare" on page 41.*

This chapter contains the following sections:


- New and Enhanced Features in ExtremeWare 7.3 on page 15
- Supported Hardware on page 24


## New and Enhanced Features in ExtremeWare 7.3

Following are descriptions of features introduced or enhanced in ExtremeWare 7.3. These features are documented in detail in the *ExtremeWare 7.3 Software User Guide* or the *ExtremeWare 7.3 Software Command Reference Guide,* unless otherwise noted.

### Cable Diagnostics

The Cable Diagnostic Module (CDM) is used to collect cable diagnostic values for the physical ports on the system. CDM is implemented as two submodules:

- DIAG submodule—Implements the diagnostic functionality of the CDM
- TMR submodule—Handles all timer related issues

### Port Aggregate Bandwidth Control

Port Aggregate Bandwidth Control is a feature designed to control aggregate bandwidth of all queues on a specific port. It is usually deployed when a customer uses several queues for classifying traffic and needs to restrict the total queue bandwidth to a specific amount.

## Standard Multinetting

Multinetting provides a way of assigning multiple subnets to a routing interface. This benefits networks that outgrow their allocated subnets. When the network grows due to a lack of address ranges in the original subnet, a new subnet is allocated. In the Extreme Networks implementation, routing interfaces can be assigned multiple subnets. IP routing occurs between the different subnets of the same interface, as well as between the subnets of different interfaces.

## PIM Snooping

In networks where a Layer 2 switch interconnects several routers, such as an Internet exchange point (IXP), the switch floods IP multicast packets on all multicast router ports by default, even if there are no multicast receivers downstream. With PIM snooping enabled, the switch restricts multicast packets for each IP multicast group to only those multicast router ports that have downstream receivers joined to that group. When you enable PIM snooping, the switch learns which multicast router ports need to receive the multicast traffic within a specific VLAN by listening to the PIM hello messages, PIM join and prune messages, and bidirectional PIM designated forwarder-election messages.

## IP Address Security

### CPU DoS Protect Enhancements

This feature allows you to manage and reduce high CPU utilization caused by an ICMP DOS attack. It will also help your reduce or eliminate the impact of such attacks on switch performance.

### SNMP Traps and MIBs for CPU DoS Protect

SNMP traps and MIBs provide access to the statistics available in the ExtremeWare Command Line Interface (CLI).

## IPDA Subnet Lookup

The Extreme Networks IPDA subnet lookup feature Increases IP address coverage in the hardware forwarding table. It makes it possible for a switch to cover the entire IP address range, from A class to C class, through setting the length of the IPDA subnet lookup mask. The expansion helps guarantee wire-speed performance in a L3 switch for all ports.

It also offers better protection of internal traffic from malicious end-users or virus infected clients. Scanning for virus-infected end users, or malicious users, can cause the FDB table to fill up quickly. The attacks can significantly hurt the quality of internal traffic if all L3 forwarding is made by only host lookup. The IPDA subnet lookup feature makes the attack traffic use the IPFDB subnet forwarding table instead of the host forwarding table. This means that internal traffic, which uses the host forwarding table can preserve the same quality when under attack.

## sFlow

sFlow is a technology for monitoring traffic in data networks containing switches and routers. In particular, it defines the sampling mechanisms implemented in an sFlow Agent for monitoring traffic, the sFlow MIB for controlling the sFlow Agent, and the format of sample data used by the sFlow Agent when forwarding data to a central data collector.

## Stand-alone ELRP

Extreme Loop Recovery Protocol (ELRP) is used to detect network loops in an L2 network. A switch running ELRP transmits multicast packets with a special MAC destination address out of some, or all, of the ports belonging to a VLAN. All the other switches in the network treat this packet as a regular, multicast packet and flood it to all the ports belonging to the VLAN. If the packets transmitted by a switch are received back by that switch, this indicates a loop in the layer-2 network. Once a loop is detected by ELRP, different recovery actions can be taken such as blocking certain ports to prevent loops, or logging a message to the system log. The action taken is largely dependent on the protocol using ELRP to detect loops in the network.

## RADIUS Server Configuration Enhancements in ExtremeWare 7.3

ExtremeWare 7.3 has added enhancements for configuring the RADIUS server:

### Configuring RADIUS Servers

In ExtremeWare 7.3, you can configure up to four RADIUS servers: two primary servers and two secondary servers. P1 and P2 indicates the two primary server settings. S1 and S2 indicates the two secondary server settings. The Default Authentication Primary and Secondary server setting for both management and network access is P1 and S1.

### Configuring RADIUS Authentication and Accounting Servers

If you set the RADIUS server for management or network access for the current session, the setting takes precedence over the default setting. If you unconfigure the setting, the default authentication setting takes effect again.

- Use the `configure auth mgmt-access` command to set up management access for the primary and secondary RADIUS servers.
- Use the `configure auth netlogin radius` command to configure a set of primary or secondary RADIUS servers for network access.

### Showing the Current RADIUS Server Authentication Setting

Use the `show auth` command to show the authentication servers configured for mgmt-access/netlogin type of sessions. If you use the `configure auth mgmt-access radius` or the `configure auth netlogin radius` command, the `show auth` command will show the session setting for the management or Network Login sessions. If both `configure auth mgmt-access radius` and `configure auth netlogin radius` commands are used, then the `show auth` command will display the session setting for both the management and Network Login sessions, and omits the Default Auth Setting.

The `show auth` command will not show anything if you are not specifically setting up authentication using the `configure auth` command and:

- RADIUS is disabled.
- P1 and S1 are not configured. In other words, you have enabled RADIUS without configuring a RADIUS server.
- P2 and S2 are configured; P1 and S1 are unconfigured. Although the `show radius` command still shows P2 and S2, by default, these RADIUS settings are not set in the default authentication.

## Configuring a RADIUS Server for Network Login Users (Wired and Wireless)

If you want to configure RADIUS for Network Login users only and do not want to configure RADIUS for management access, do the following:

1. Configure the first primary or secondary RADIUS server.
2. Configure the second primary or secondary RADIUS server using a fictitious IP address.
3. Configure authentication to the fictitious IP address using the `config auth mgmt-access radius` command.
4. Login to the switch. RADIUS authentication will always fail, causing the switch to time out and go to the local account. Authentication is performed at the local account.

## Management Access with RADIUS Enabled

Switch management access must use RADIUS for authentication when RADIUS is enabled on the switch.

**Workaround:** If you want to use local authentication for management access, you should configure invalid RADIUS servers (both primary and secondary) for management access. This will cause RADIUS authentication to timeout and fall back to local authentication. This feature works as designed today and will be enhanced in a future release.

**RADIUS Examples**

**Example 1:**

```
config radius primary server 10.201.30.8 client-ip 10.201.56.3
config radius secondary server 10.201.30.9 client-ip 10.201.56.3
config radius primary server 1.1.1.1 client-ip 10.201.56.3
config radius primary shared-secret secret
config radius secondary shared-secret secret
enable radius
configure auth netlogin radius primary 10.201.30.8 secondary 10.201.30.9
config auth mgmt-access radius primary 1.1.1.1

Output 1:

* mars:32 # show radius
Radius: enabled
Primary Radius server shared-secret "qijxou"
Secondary Radius server shared-secret "qijxou"
Radius Server Connect Timeout sec 3
Radius servers:
  Server name:     10.201.30.8
  Server type:     Primary
  IP address:      10.201.30.8
  Server IP Port:  1645
  Client address:  10.201.56.3
  Radius Server Connect Timeout sec:   3
  Shared secret:  qijxou
  Access Requests:     0      Access Accepts:      0     Access Rejects:   0
  Access Challenges:   0      Access Retransmits:  0     Client timeouts:  0
  Bad authenticators:  0      Unknown types:       0     Round Trip Time:  0 sec(s)


  Server name:     10.201.30.9
  Server type:     Secondary
```

```
  IP address:      10.201.30.9
  Server IP Port:  1645
  Client address:  10.201.56.3
  Radius Server Connect Timeout sec:   3
  Shared secret:  qijxou
  Access Requests:     0      Access Accepts:      0     Access Rejects:   0
  Access Challenges:   0      Access Retransmits:  0     Client timeouts:  0
  Bad authenticators:  0      Unknown types:       0     Round Trip Time:  0 sec(s)


  Server name:      1.1.1.1
  Server type:      Primary
  IP address:       1.1.1.1
  Server IP Port:  1645
  Client address:  10.201.56.3
  Radius Server Connect Timeout sec:   3
  Shared secret:  qijxou
  Access Requests:     6      Access Accepts:       0           Access Rejects:0
  Access Challenges:   0    Access Retransmits:      6     Client timeouts:   2
  Bad authenticators:  0    Unknown types:     0  Round Trip Time:  42949672 sec(s)


Radius Accounting: disabled
Radius Acct Server Connect Timeout sec 3
Primary radius accounting servers:    Not configured
Secondary radius accounting servers:  Not configured


* mars:33 # show auth
Session Type : mgmt-access
  Authentication Server Type       :  Radius
  Primary Authentication Server    :  1.1.1.1
  Secondary Authentication Server  :  None
  Primary Accounting Server        :  None
  Secondary Accounting Server      :  None
Session Type : netlogin
  Authentication Server Type       :  Radius
  Primary Authentication Server    :  10.201.30.8
  Secondary Authentication Server  :  10.201.30.9
  Primary Accounting Server        :  None
  Secondary Accounting Server      :  None
* mars:34 #
```

**Example 2:**

```
config radius primary server 10.201.30.8 client-ip 10.201.56.3
config radius secondary server 10.201.30.9 client-ip 10.201.56.3
config radius primary shared-secret secret
config radius secondary shared-secret secret
enable radius
configure tacacs primary server 1.1.1.1 client-ip 10.201.56.3
config tacacs primary shared-secret secret
enable tacacs
configure auth netlogin radius primary 10.201.30.8 secondary 10.201.30.9
config auth mgmt-access tacacs primary 1.1.1.1
```

```
Output 2:

* mars:36 # show auth
Session Type : mgmt-access
  Authentication Server Type       :  Tacacs
  Primary Authentication Server    :  1.1.1.1
  Secondary Authentication Server  :  None
  Primary Accounting Server        :  None
  Secondary Accounting Server      :  None
Session Type : netlogin
  Authentication Server Type       : Radius
  Primary Authentication Server    : 10.201.30.8
  Secondary Authentication Server  : 10.201.30.9
  Primary Accounting Server        : None
  Secondary Accounting Server      : None
* mars:37 #
```

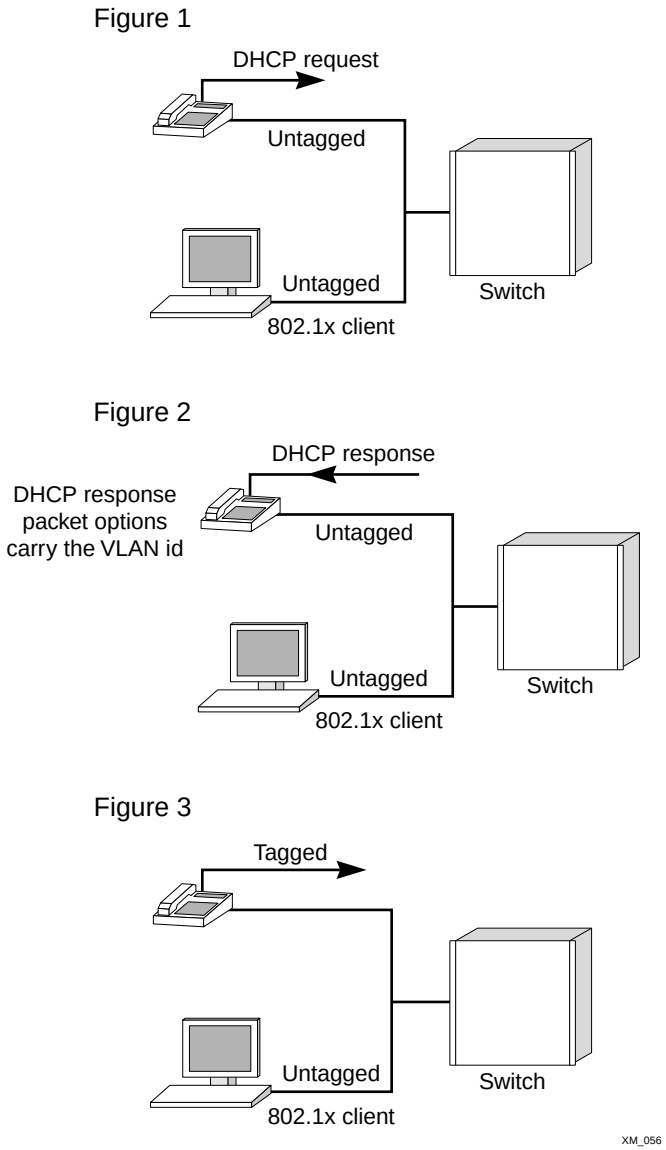
## Trusted Organizational Unique Identifier

The Trusted Organizational Unique Identifier (OUI) feature allows devices, such as IP phones, without 802.1x (Network Login) capability to obtain IP addresses through DHCP on a network login enabled port.

A trusted OUI configuration requires an IP phone and a desktop PC, both of which are connected to a single wired port on an Extreme Networks switch. The desktop PC must use untagged 802.1x authentication. The IP phone must be capable of sending DHCP requests after booting up to obtain IP address and VLAN ID through the DHCP response. The phone then configures itself to be tagged for the VLAN ID obtained through the DHCP response.

Figure 1 shows the sequence of operation for the trusted OUI feature.

**Figure 1:** Trusted OUI sequence of operation




## Trusted OUI and Trusted MAC CLI Commands

The switch forwards packets based on the MAC addresses, independent of the 802.1x port state. Prior to this feature, a network login enabled port cannot be part of a different tagged VLAN. This does not apply if the trusted MAC feature is enabled on both a global and a VLAN basis.

New CLI commands have been introduced to configure this feature. The following describes each command:

- Use the `create trusted-mac-address` command to configure a trusted MAC -address. The `mask` keyword is optional. If you do not specify a mask, the default mask of ff:ff:ff:ff:ff:ff is used. If you do not specify a port list, the trusted MAC is applied to all of the ports in the VLAN. Devices matching a created trusted-OUI list are allowed to bypass network login using a specified protocol.

```
create trusted-mac-address <xx:yy:zz:aa:bb:cc> {mask dd:ee:ff:gg:hh:kk>} vlan
<vlan-name | all> {port <port-list>} {protocol[DHCP|ARP]}
```

- Use the `delete trusted-mac-address` to delete a MAC address. If you do not specify the MAC address to be deleted, all the MAC addresses in the VLAN are deleted.

  ```
  delete trusted-mac-address {mac-address <xx:yy:zz:aa:bb:cc> {mask
  <dd:ee:ff:gg:hh:kk>}} vlan <vlan-name | all> {ports <port-list>}
  {protocol[DHCP|ARP]}
  ```

- Use the `disable trusted-mac-address` command to disable trusted OUI or MAC addresses for port-specific configurations. Disabling this feature will not remove the previous port-specific configurations.

  ```
  disable trusted-mac-address {vlan <vlan-name>}
  ```

- Use the `enabled trusted-mac-address` command to enable trusted OUI or MAC addresses for port-specific configurations. Disabling this feature will not remove the previous port-specific configurations. The system default is `disable trusted-mac-address`.

  ```
  enabled trusted-mac-address
  ```

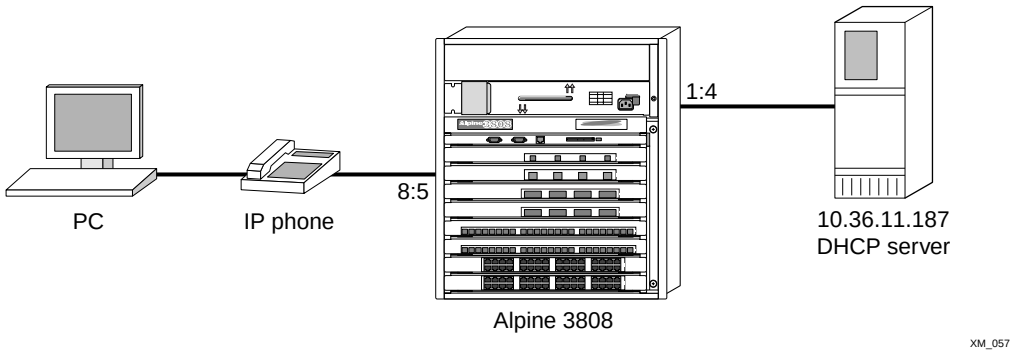
  The global trusted MAC feature should be enabled globally and also with a VLAN for this feature to be effective.

  ```
  enabled trusted-mac-address {vlan <vlan-name>}
  ```

- Use the `show trusted-mac-address` command to display the status of the enable/disable keywords and then displays all of the configured trusted MAC addresses.

  ```
  show trusted-mac-address {vlan <vlan-name>} {port <port-list>}
  ```

**Figure 2:** show trusted-mac-address Command Sequence




Command sequence

```
create vlan "voice"
configure vlan "voice" tag 120
configure vlan "voice" ipaddress 20.36.11.1 255.255.255.0
configure vlan "voice" add port 8:5 tagged
enable ipforwarding vlan "voice"

create vlan "corp"
configure vlan "corp" tag 9
configure vlan "corp" ipaddress 10.36.11.186 255.0.0.0
configure vlan "corp" add port 8:5 untagged
configure vlan "corp" add port 1:4 tagged
enable ipforwarding vlan "corp"

enable netlogin port 8:5 vlan corp

create trusted-mac-address mac-address 00:04:0D:28:45:C2 mask FF:FF:FF:FF:FF:FF
corp ports 8:5 protocol dhcp
enable trusted-mac-address
enable trusted-mac-address vlan corp

enable bootprelay
configure bootprelay add 10.36.11.187
```

## Link Aggregation Control Protocol (LACP)

LACP is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.

Table 1 lists the modules and interface cards used for testing LACP on ExtremeWare 7.3.

**Table 1:** LACP Testing Matrix, Alpine Modules and NICs

| Alpine 3804 | Module 1 FM32T | Module 2 G4Tx | Module 4 G16Tx | Module 4 G4X |
|---|---|---|---|---|
| **Server NICs** | | | | |
| Built-in Intel 10/100 | X* | X | X | N/A |
| Intel PRO/1000 MTx | X | X | X | N/A |
| Intel PRO/1000 MF | N/A | N/A | NA | X |

*The built-in 10/100 NIC experienced some link problems when connecting to the FM32T.

## Unified Access Feature Support

ExtremeWare 7.3 supports the following unified access features:

- Wireless network login
- Inter-Access Point Protocol (IAPP), which provides seamless roaming support for data and voice clients
- Spectralink Voice Protocol (SVP) support for voice over WLAN Spectralink handsets
- Wireless monitoring (AP Scan, Client Scan, Client Statistics)
- Comprehensive wireless security support with WPA/AES
- MAC-RADIUS support for wireless data clients
- Extensive debugging support (MAC, RADIUS, dot1x, WPA, IAPP, AP-Management, and so on)

To use the UAA and PoE features, you must be running the v732b3.xtr or v732b3.Sxtr image.

## New .Bxtr Software Image

ExtremeWare 7.3 offers two software images: .xtr and .Bxtr. The .Bxtr software image is available on all Summit platforms. It does not support the following features:

- UAA (available on Alpine switches only)
- PoE (available on Alpine switches only)
- SSL (HTTPS)

Although the BlackDiamond 6804 and BlackDiamond 6808 switches use the .xtr software image, the BlackDiamond switches do not support UAA and PoE.

To use SMA and SONET the advanced image (.xtr or Sxtr) must be used (PD3-10674849 and PD3-10693717).

# Supported Hardware

Hardware in the following sections listed in *italics* is new for this release.

ExtremeWare 7.3 (and later) supports "*i*" series or "e" series products *only*.

Table 2 lists software filenames for the hardware that requires software.

**Table 2:** Software for supported hardware

| Extreme Hardware | ExtremeWare Filename | BootROM Filename/Version |
|---|---|---|
| BlackDiamond 6816 | v732b3.Gxtr or v732b3.SGxtr | Ngboot8.2.bin/8.2 |
| BlackDiamond 6808 | v732b3.xtr or v732b3.Sxtr | Ngboot8.2.bin/8.2 |
| BlackDiamond 6804 | v732b3.xtr or v732b3.Sxtr | Ngboot8.2.bin/8.2 |
| Alpine 3808 | v732b3.xtr or v732b3.Sxtr | Ngboot8.2.bin/8.2 |
| Alpine 3804 | v732b3.xtr or v732b3.Sxtr | Ngboot8.2.bin/8.2 |
| Alpine 3802 | v732b3.xtr or v732b3.Sxtr/EW-70-3802.mig | Ngboot8.2.bin/8.2 |
| Summit7i/7iT | v732b3.Bxtr or v732b3.SBxtr | Ngboot8.2.bin/8.2 |

**Table 2:** Software for supported hardware (continued)

| Extreme Hardware | ExtremeWare Filename | BootROM Filename/Version |
|---|---|---|
| Summit1i/1iT | v732b3.Bxtr or v732b3.SBxtr | Ngboot8.2.bin/8.2 |
| Summit5i/5iT/5iLX | v732b3.Bxtr or v732b3.SBxtr | Ngboot8.2.bin/8.2 |
| Summit48i | v732b3.Bxtr or v732b3.SBxtr | Ngboot8.2.bin/8.2 |
| Summit48si | v732b3.Bxtr or v732b3.SBxtr | Ngboot8.2.bin/8.2 |
| ARM module | v732b3.arm | v732b3.nprom/1.18 |
| OC3 PoS module | v732b3.oc3 | v732b3.nprom/1.18 |
| OC12 PoS module | v732b3.oc12 | v732b3.nprom/1.18 |
| OC3 ATM module | v732b3.atm3 | v732b3.nprom/1.18 |
| MPLS module | v732b3.mpls | v732b3.nprom/1.18 |
| T1 module | v732b3.t1 | t1boot28.wr/2.8 |
| E1 module | v732b3.e1 | e1boot28.wr/2.8 |
| T3 module | v732b3.t3 | t3boot28.wr/2.8 |

**NOTE**

*The BlackDiamond 6816 requires its own ExtremeWare image. The image that runs on other BlackDiamond, Alpine, or stackable switches does not support the BlackDiamond 6816.*

**NOTE**

*Systems with 128 MB memory should use the v732b3.Bxtr or v732b3.SBxtr image. To determine how much memory is available, use the* `show memory` *command.*

## BlackDiamond Component Support

BlackDiamond components supported with ExtremeWare 7.3, and the minimum ExtremeWare version required by the chassis to support each component, include:

**Table 3:** BlackDiamond component support

| BlackDiamond Component | ExtremeWare Required |
|---|---|
| BlackDiamond 6804 | 6.2.2b56[1] |
| BlackDiamond 6808 | 6.2.2b56[1] |
| BlackDiamond 6816 | 6.2.2b56[1] |
| MSM-3 | 7.1.1 |
| MSM64i | 6.2.2b56[1] |
| G8Xi | 6.1.3 |
| G8Ti | 6.1.3 |
| G12SXi | 6.1.4 |
| G16X[3] | 7.0.1 |
| G24T[3] | 7.0.1 |
| F32Fi | 6.1.8 |

**Table 3:** BlackDiamond component support (continued)

| BlackDiamond Component | ExtremeWare Required |
|---|---|
| F48Ti | 6.1.2 |
| F96Ti | 6.1.8 |
| WDMi | 6.1.5 |
| 10GLRi | 7.0 |
| 10GX3 | 7.2.0b18 |
| MPLS | 7.0 |
| ARM | 7.0 |
| P3cMi | 7.0 |
| P3cSi | 7.0 |
| P12cMi | 7.0 |
| P12cSi | 7.0 |
| A3cMi | 7.0 |
| A3cSi | 7.0 |
| DC Power Supply | 6.1.5 |
| 110 VAC Power Supply | 6.1.5 |
| 220 VAC Power Supply | 6.1.5 |

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

**NOTE**

*Do not install mixed versions of the power supplies in the same system. Install power supplies of the same type.*

## Alpine Component Support

Alpine components supported with ExtremeWare 7.3, and the minimum ExtremeWare version required, include:

**Table 4:** Alpine component support

| Alpine Component | ExtremeWare Required |
|---|---|
| Alpine 3802 | 6.2.2b56[1] |
| Alpine 3804 | 6.2.2b56[1] |
| Alpine 3808 | 6.2.2b56[1] |
| SMMi | 6.2.2b56[1] |
| GM-4Si/Xi/Ti | 6.1.5 |
| GM-16X[3] | 7.0.1 |
| GM-16T[3] | 7.0.1 |
| FM-32Ti | 6.1.5 |
| FM-24MFi | 6.1.5 |

**Table 4:** Alpine component support (continued)

| Alpine Component | ExtremeWare Required |
|---|---|
| FM-24Ti | 6.1.7 |
| FM-24SFi | 6.1.7 |
| FM-32Pi | 7.2.0b18 |
| GM-WDMi | 6.1.8 |
| WM-4T1i | 7.0.1 |
| WM-4E1i | 7.0.1 |
| WM-1T3i | 7.0.1 |
| FM-8Vi | 7.0.1 |
| AC Power Supply | 6.1 |
| DC Power Supply | 6.1.5 |

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

## Summit Component Support

Summit components supported with ExtremeWare 7.3, and the minimum ExtremeWare version required, include:

**Table 5:** Summit component support

| Summit Component | ExtremeWare Required |
|---|---|
| Summit1i | 6.2.2b56[1] |
| Summit5i | 6.2.2b56[1] |
| Summit7i | 6.2.2b56[1] |
| Summit7i DC Power Supply | 6.2.2b56[1] |
| Summit48i | 6.2.2b56[1] |
| Summit48si | 6.2.2b56[1] |
| Summit48si DC Power Supply | 7.1.1[2] |

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.
2. ExtremeWare 6.2.2 recognizes the Summit48si DC power supply, but does not indicate the type of PSU installed, issue a warning if both an AC and a DC PSU are installed in the same chassis, or send an SNMP trap message when the PSU is hot-swapped.

## GBIC Support

GBICs supported with ExtremeWare 7.3, and the minimum ExtremeWare version required, include:

**Table 6:** GBIC support

| GBIC | ExtremeWare Required |
|---|---|
| SX parallel ID | 1.0 |
| SX serial ID | 2.0 |
| LX parallel ID | 1.0 |
| LX serial ID | 2.0 |
| ZX | 6.2.2 |
| ZX Rev 03 | 6.2.2 |
| LX70 | 2.0 |
| LX100 | 6.1.9 |
| UTP | 6.1.9 |
| SX Mini | 7.0.1b11 |
| LX Mini | 7.0.1b11 |
| ZX Mini | 7.0.1b11 |

The following table describes how each version of ExtremeWare interprets the media type of the installed GBIC, based on either the Vista web interface, or the `show port configuration` command. All versions correctly identify Parallel ID GBIC types; however, some versions do not correctly identify the Serial ID GBIC type because the Serial ID GBICs were introduced after the software was released.

**Table 7:** ExtremeWare recognition of GBIC type

| ExtremeWare Version | SX Parallel ID | LX Parallel ID | SX Serial ID | LX Serial ID | LX70 |
|---|---|---|---|---|---|
| 1.x | SX | LX | Not Supported | Not Supported | Not Supported |
| 2.x | SX | LX | LX | LX | LX |
| 3.x | SX | LX | CX | CX | CX |
| 4.x | SX | LX | SX | LX | LX |
| 6.x | SX | LX | SX | LX | LX70 (6.1.6 and above) |
| 7.x | SX | LX | SX | LX | LX70 |

### Mini-GBIC Support

Extreme products support the Extreme mini-GBIC only. For reliability and stability reasons, third-party mini-GBICs are not supported at this time.

## XENPAK Module Support

XENPAK modules supported with ExtremeWare 7.3, the minimum ExtremeWare version required, and the manufacturers supported include:

**Table 8:** XENPAK support

| XENPAK Module | ExtremeWare Required | Manufacturers Supported |
|---|---|---|
| LR | 7.2.0b18 | Intel, Opnext |
| ER | 7.2.0b18 | Intel, Opnext |

# Channel Mapping

Table 9 lists the channel mapping for Altitude 300-2i wireless ports connected to a Alpine 3800 series switch using ExtremeWare 7.3. The UAA features contained in this table apply to Alpine 3800 switches only.

**Table 9:** Altitude 300-2i channel mapping

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Canada | CA | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Hong Kong | HK | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| United States | US | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Japan | JP | 34/38/42/46 | 1-13 | 1-14 |
| Argentina | AR | 56/60/64/149/153/157/161 | 1-13 | 1-13 |
| Australia | AU | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-13 | 1-13 |
| Austria | AT | 36/40/44/48 | 1-13 | 1-13 |
| Belgium | BE | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Brazil | BR | 36/40/44/48/149/153/157/161/165 | 1-13 | 1-13 |
| Chile | CL | 149/153/157/161/165 | 1-13 | 1-13 |
| China | CN | 149/153/157/161/165 | 1-13 | 1-13 |
| Colombia | CO | 36/40/44/46/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Costa Rica | CR | None | 1-13 | 1-13 |
| Cyprus | CY | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Czech Republic | CZ | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Denmark | DK | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Egypt | EG | None | 1-13 | 1-13 |
| Estonia | EE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Finland | FI | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| France | FR | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |

**Table 9:** Altitude 300-2i channel mapping (continued)

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Germany | DE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Greece | GR | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Hungary | HU | 36/40/44/48 | 1-13 | 1-13 |
| Iceland | IS | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| India | IN | None | 1-13 | 1-13 |
| Indonesia | ID | None | 1-13 | 1-13 |
| Ireland | IE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Israel | IL | None | 1-13 | 1-13 |
| Italy | IT | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Jordan | JO | None | 1-13 | 1-13 |
| Korea ROC (south) | KR | 149/153/157/161 | 1-13 | 1-13 |
| Kuwait | KW | None | 1-13 | 1-13 |
| Latvia | LV | None | 1-13 | 1-13 |
| Liechtenstein | LI | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Lithuania | LT | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Luxembourg | LU | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Malaysia | MY | 52/56/60/64/149/153/157/161 | 1-11 | 1-11 |
| Mexico | MX | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Netherlands | NL | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| New Zealand | NZ | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-13 | 1-13 |
| Norway | NO | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Poland | PL | 36/40/44/48/52/56/60/64100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Portugal | PT | 36/40/44/48/52/56/60/64100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Puerto Rico | PR | 36/40/44/48/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Russia | RU | None | 1-13 | 1-13 |
| Saudi Arabia | SA | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Singapore | SG | 36/40/44/48/149/153/157/161/165 | 1-13 | 1-13 |
| Slovak Republic | SK | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Slovenia | SI | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| South Africa | ZA | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

**Table 9:** Altitude 300-2i channel mapping (continued)

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Spain | SP | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Sweden | SE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Switzerland | CH | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Taiwan | TW | 56/60/64/149/153/157/161 | 1-11 | 1-11 |
| Thailand | TH | 149/153/157/161 | 1-13 | 1-13 |
| Turkey | TR | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| United Arab Emirates | AE | None | 1-13 | 1-13 |
| United Kingdom | GB | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

Table 10 lists the channel mapping for indoor Altitude 300-2d wireless ports connected to an Alpine 3800 switch using ExtremeWare 7.3.

**Table 10:** Altitude 300-2d indoor channel mapping

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Canada | CA | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Hong Kong | HK | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| United States | US | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Japan | JP | 34/38/42/46 | 1-13 | 1-14 |
| Argentina | AR | 56/60/64 | None | 1-13 |
| Australia | AU | 52/56/60/64/149/153/157/161 | 1-13 | 1-13 |
| Austria | AT | 36/40/44/48 | 1-13 | 1-13 |
| Belgium | BE | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Brazil | BR | 149/153/157/161/165 | 1-13 | 1-13 |
| Chile | CL | 149/153/157/161/165 | None | 1-13 |
| China | CN | 149/153/157/161/165 | 1-13 | 1-13 |
| Colombia | CO | 36/40/44/46/52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Costa Rica | CR | None | 1-13 | 1-13 |
| Cyprus | CY | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Czech Republic | CZ | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Denmark | DK | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Egypt | EG | None | 1-13 | 1-13 |
| Estonia | EE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Finland | FI | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

**Table 10:** Altitude 300-2d indoor channel mapping (continued)

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| France | FR | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Germany | DE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Greece | GR | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Hungary | HU | 36/40/44/48 | 1-13 | 1-13 |
| Iceland | IS | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| India | IN | None | 1-13 | 1-13 |
| Indonesia | ID | None | 1-13 | 1-13 |
| Ireland | IE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Israel | IL | None | 1-13 | 1-13 |
| Italy | IT | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Jordan | JO | 36/40/44/48 | 1-13 | 1-13 |
| Korea ROC (south) | KR | 149/153/157/161 | 1-13 | 1-13 |
| Kuwait | KW | None | 1-13 | 1-13 |
| Latvia | LV | None | 1-13 | 1-13 |
| Liechtenstein | LI | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Lithuania | LT | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Luxembourg | LU | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Malaysia | MY | 52/56/60/64/149/153/157/161 | 1-11 | 1-11 |
| Mexico | MX | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Netherlands | NL | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| New Zealand | NZ | 52/56/60/64/149/153/157/161/165 | 1-13 | 1-13 |
| Norway | NO | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Poland | PL | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Portugal | PT | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Puerto Rico | PR | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Russia | RU | None | 1-13 | 1-13 |
| Saudi Arabia | SA | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Singapore | SG | 149/153/157/161/165 | 1-13 | 1-13 |
| Slovak Republic | SK | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Slovenia | SI | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

**Table 10:** Altitude 300-2d indoor channel mapping (continued)

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| South Africa | ZA | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Spain | SP | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Sweden | SE | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Switzerland | CH | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| Taiwan | TW | 56/60/64/149/153/157/161 | 1-11 | 1-11 |
| Thailand | TH | 149/153/157/161 | 1-13 | 1-13 |
| Turkey | TR | 36/40/44/48/52/56/60/64 | 1-13 | 1-13 |
| United Arab Emirates | AE | None | 1-13 | 1-13 |
| United Kingdom | GB | 36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

Table 11 lists the channel mapping for outdoor Altitude 300-2d wireless ports connected to an Alpine 3800 switch using ExtremeWare 7.3.

**Table 11:** Altitude 300-2d outdoor channel mapping

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Canada | CA | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Hong Kong | HK | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| United States | US | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Japan | JP | None | 1-13 | 1-14 |
| Argentina | AR | 56/60/64/149/153/157/161 | 1-13 | 1-13 |
| Australia | AU | 52/56/60/64/149/153/157/161/165 | 1-13 | 1-13 |
| Austria | AT | None | 1-13 | 1-13 |
| Belgium | BE | None | 1-13 | 1-13 |
| Brazil | BR | 149/153/157/161/165 | 1-13 | 1-13 |
| Chile | CL | 149/153/157/161/165 | None | 1-13 |
| China | CN | 149/153/157/161/165 | 1-13 | 1-13 |
| Colombia | CO | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Costa Rica | CR | None | 1-13 | 1-13 |
| Cyprus | CY | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Czech Republic | CZ | None | 1-13 | 1-13 |
| Denmark | DK | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Egypt | EG | None | 1-13 | 1-13 |
| Estonia | EE | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Finland | FI | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| France | FR | None | 1-7 | 1-7 |
| Germany | DE | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

**Table 11:** Altitude 300-2d outdoor channel mapping (continued)

| Country | Country Code | 802.11a Channels | 802.11g Channels | 802.11b Channels |
|---|---|---|---|---|
| Greece | GR | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Hungary | HU | None | 1-13 | 1-13 |
| Iceland | IS | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| India | IN | None | 1-13 | 1-13 |
| Indonesia | ID | None | 1-13 | 1-13 |
| Ireland | IE | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Israel | IL | None | 1-13 | 1-13 |
| Italy | IT | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Jordan | JO | None | 1-13 | 1-13 |
| Korea ROC (south) | KR | 149/153/157/161 | 1-13 | 1-13 |
| Kuwait | KW | None | 1-13 | 1-13 |
| Latvia | LV | None | 1-13 | 1-13 |
| Liechtenstein | LI | None | 1-13 | 1-13 |
| Lithuania | LT | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Luxembourg | LU | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Malaysia | MY | 52/56/60/64/149/153/157/161 | 1-11 | 1-11 |
| Mexico | MX | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Netherlands | NL | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| New Zealand | NZ | 52/56/60/64/149/153/157/161/165 | 1-13 | 1-13 |
| Norway | NO | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Poland | PL | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Portugal | PT | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Puerto Rico | PR | 52/56/60/64/149/153/157/161/165 | 1-11 | 1-11 |
| Russia | RU | None | 1-13 | 1-13 |
| Saudi Arabia | SA | None | 1-13 | 1-13 |
| Singapore | SG | 149/153/157/161/165 | 1-13 | 1-13 |
| Slovak Republic | SK | None | 1-13 | 1-13 |
| Slovenia | SI | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| South Africa | ZA | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Spain | SP | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Sweden | SE | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |
| Switzerland | CH | None | 1-13 | 1-13 |
| Taiwan | TW | 149/153/157/161 | 1-11 | 1-11 |
| Thailand | TH | 149/153/157/161 | 1-13 | 1-13 |
| Turkey | TR | None | 1-13 | 1-13 |
| United Arab Emirates | AE | None | 1-13 | 1-13 |
| United Kingdom | GB | 100/104/108/112/116/120/124/128/132/136/140 | 1-13 | 1-13 |

# Tested Third-Party Products

This section lists the third-party products tested for Alpine 3800 switches. The UAA features contained in this section apply to Alpine 3800 switches only.

## Tested NICs

The wireless NICs in Table 12, Table 13, Table 14, Table 15, and Table 16 are tested with the listed software (or later) and authentication method.

**Table 12:** 802.11 a/b/g wireless NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Proxim A/B/G Gold | 2.4.2.1.7<br>2.3.0.75 | W2K SP4<br>WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS |
| NetGear WAG511 | 2.4.1.1.30<br>2.3.0.73 | W2K SP4<br>WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS |
| D-link DWL-AG650 Airpro | 2.0.1.254 | W2K SP4<br>WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |
| D-link DWL-AG650<br>AirExpert AG660 | 2.1.3.1 | WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS |
| 3Com 3CRWE154A72 | 2.4.1.3.3 | W2K SP4<br>WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS |
| Linksys AG WPC55AG | 2.3.2.4 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS<br>PEAP/TLS |
| Cisco Air-CB21AG | 1.0.0.305 | | Card Utility | PEAP/TLS |

**Table 13:** 802.11 a/b wireless NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Linksys WPC51AB | 2.0.1.254 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |
| Orinoco Gold A/B | 7.64.1.316 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |

**Table 14:** 802.11a wireless NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Cisco 11a-only Air-CB20A | 3.4.19.0 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS<br>PEAP/TLS |

**Table 15:** 802.11b wireless NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Cisco Aironet350 b | 8.1.6.0 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS |
| Netgear MA401 b-only | 2.0.2.0 | W2K SP4 | Odyssey 2.2/Card Utility | PEAP/TLS<br>PEAP/TLS |
| Microsoft b card MN520 | D-link 2.0.1.254 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS<br>PEAP/TLS |
| 3Com 11b-only 3CRWE60292B | 2.1.1.3005 | W2K SP4<br>WinXP SP1 | Odyssey 2.2/Card Utility | PEAP/TLS<br>PEAP/TLS/TTLS |

**Table 16:** 802.11g wireless NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| NetGear WG511 | 2.1.1.4 | | Odyssey 2.2 | PEAP/TLS |
| Dell True Mobile 1300 | 3.20.23.0 | | Odyssey/Card Utility | PEAP/TLS |
| Buffalo WLI-CB-G54 | 3.10.53.6 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |
| Linksys WPC54G | 3.20.21.0 | WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| D-link DWL G650Airplus | 1.0.0.5 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |
| D-Link 11g-only DWL-G650-B2 | 2.1.3.1 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |
| Microsoft MN-720 | 3.20.26.0 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS<br>PEAP/TLS/TTLS |

**Table 17:** 802.11g MiniPCI wireless NIC

| NIC | Driver | OS | Third-Party Software | Third-Party Software |
|---|---|---|---|---|
| Broadcom 54G MaxPerformance | 3.20.23.0 | | Card Utility | Odyssey 2.2 |

The wireless PCI cards in Table 18 are tested with the listed software (or later) and authentication method.

**Table 18:** Wireless PCI cards

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Linksys WMP54G | 3.30.15.0 | W2K SP4 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS |
| NetGear WAG311 Tri-mode | 2.4.0.72 | W2K SP4 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS |
| NetGear WG311 | 2.4.0.71 | W2K SP4 | Odyssey 2.2/Card Utility | PEAP/TLS/TTLS |

### WPA-Compliant Wireless NICs

The wireless NICs in Table 19, Table 20, and Table 21 are WPA-compliant.

**NOTE**

*WPA compliant wireless NICs support TKIP and AES with pre-shared and dynamic keys.*

**Table 19:** Wireless tri-mode NICs

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| NetGear WAG511 | 2.3.0.73 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| D-link DWL-AG650 AirExpert | 1.2.0.1 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| 3Com 3CRWE154A72 | 2.4.1.33 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| 3Com 3CRPAG175 | 1.0.0.25 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| Proxim A/B/G | 2.4.2.1.7 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| D-Link AG660 | 2.1.3.1 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| Linksys AG WPC55AG | 2.3.2.4 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| Cisco Air-CB21AG | 1.0.0.305 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS |

**Table 20:** Wireless 802.11g NICs (WPA compliant)

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| Buffalo WLI-CB-G54 | 3.10.53.6 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| NetGear WG511T | 3.0.0.43 | | Odyssey | PEAP/TLS/TTLS |
| Linksys WPC54G | 3.20.21.0 | WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| D-Link DWL-G650-B2 | 1.0.0.5 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| Microsoft MN-720 | 3.20.21.0 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |

**Table 21:** Wireless 802.11 a/b NICs (WPA compliant)

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| D-link AirPro AB650 | 2.4.0.73 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |

**Table 21:** Wireless 802.11 a/b NICs (WPA compliant)

| NIC | Driver | OS | Third-Party Software | Authentication Method |
|---|---|---|---|---|
| NetGear WAB501 | 2.4.0.71 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |
| Avaya Platinum A/B | 2.4.1.21 | W2K SP4<br>WinXP SP1 | Odyssey 2.2 | PEAP/TLS/TTLS |

## Tested RADIUS Servers

These RADIUS servers are fully tested:

- Microsoft Internet Authentication Server
- Funk Steel Belted RADIUS Enterprise Edition 4.5
- Meeting House
- Free Radius
- InfoBlox RadiusONE
- Roving Planet
- Cisco ACS

## Tested Third-Party Clients

These third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.00.0.937

## Tested Laptops

These laptops are fully tested:

- IBM Thinkpad T40 (Intel Centrino-based 802.11b)
- IBM Thinkpad T41 (Intel Centrino-based 802.11b)
- Dell Latitude D800 (Intel Centrino-based 802.11b)
- HP/Compaq nx9010 (Broadcom 54G MaxPerformance MiniPCI)
- Fujitsu Lifebook N series (Broadcom 54G MaxPerformance MiniPCI)
- Sony PCG-K15
- Dell Latitude D600

## Tested PDAs

These PDAs are fully tested:

- iPAQ H5550
- Dell Axim x3i
- HP Pocket PC 4155

## Tested Tablets

These tablets are fully tested:

- NEC Tablet

## Tested Scanner

The following scanner is fully tested:

- Intermec Scanner Model 700 Color-Pocket PC - 802.11b CF: Open Authentication/No encryption, Shared/WEP, and Open/WEP

## Tested IP Phones

These IP phones are fully tested:

- Symbol Netvision IP-Phone

## Tested Embedded WNIC Modules

- Dell Truemobile 1200, 1300, 1350, 1450
- IBM Thinkpad T40p Trimode (Centrino card)

## Tested Spectralink Supported Handsets

- Avaya 3606
- Spectralink Netlink 1640

## Tested Spectralink Gateway

- Netlink SVP Avaya Voice Priority Processor
- Netlink SVP100 Gateway

## Legacy IP Phones

These wired IP phones have been verified for PoE power up only:

- Avaya 4610SW IP
- Avaya 4620 IP New 03-016A/B
- Avaya 4620SW IP
- Super tex PD1 v1
- Super PD+PS
- TI PTB48540 CL003ENG
- 3COM NJ105
- 3COM NJ220
- 3COM NJ200 Old
- 3COM NJ200 New

- 3COM NJ100 New
- 3COM NJ100 Old
- 3COM 3C10248B with 3CNJVOIPMOD-NBX
- 3COM 3C10248PE IP Phone
- 3COM 3C10226PE IP Phone
- Avaya 4602SW IP Phone
- Avaya 4620 IP Phone
- Avaya 4630SW IP Phone
- Polycom IP 300 With 2457-11077-002 Rev.X1
- Polycom IP 500 With 2457-11077-002 Rev.X1
- Polycom IP 600
- Polycom Speaker IP 3500 with Cisco PIM
- Polycom Speaker IP 3500 with IEEE
- Linear CD671
- 3COM 655003403 PD with 3CNJVOIPMOD-NBX
- Avaya 4602 IP Phone
- Linear LTC4257IS8 with 4257
- Linear Edge PD
- TPS2375 Eval Chip #22
- TPS2375 Eval Chip #20
- Siemens Optipoint 410 Standard FV
- Siemens Optipoint 410 Entry FV
- Polycom SoundPoint IP LAN/Power Cable

## Legacy Phones with Dongle

- Cisco 7910
- Cisco 7940
- Cisco 7960
- Cisco 7970

# 2 Upgrading to ExtremeWare 7.3

This chapter contains the following sections:


- Staying Current on page 41
- Upgrading ExtremeWare on page 41
- Downgrading Switches on page 48


## Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site:

http://www.extremenetworks.com/go/esupport.htm.

## Upgrading ExtremeWare

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2b56 (or later). You can only load ExtremeWare 6.2.2 on a switch running ExtremeWare 6.1.9 (or later). Table 22 lists the BootROM required for each version of ExtremeWare.

**Table 22:** Required BootROM versions

| ExtremeWare Version | BootRom Version |
|---|---|
| ExtremeWare 7.3.0 and later | BootROM 8.2 (or later) |
| ExtremeWare 7.1.1 through ExtremeWare 7.2.0 | BootROM 8.1 (or later) |
| ExtremeWare 7.0.0 through ExtremeWare 7.1.0 | BootROM 7.8 (or later) |
| ExtremeWare 6.2.2 through ExtremeWare 6.2.2 | BootROM 7.8 |
| ExtremeWare 6.1.8 through ExtremeWare 6.2.1 | BootROM 7.2 (or later) |
| ExtremeWare 6.1 through ExtremeWare 6.1.7 | BootROM 6.5 |

If your switch is running ExtremeWare 6.1.8 (or earlier), you must first upgrade to ExtremeWare 6.1.9, then upgrade to ExtremeWare 6.2.2b56 (or later). Following are specific instructions on upgrading to, and downgrading from, ExtremeWare 7.3 for Summit, Alpine, and BlackDiamond switches.

## PoE Firmware Upgrade

**WARNING!**

*ExtremeWare 7.3.2 contains a PoE firmware upgrade for the Alpine FM-32Pi module. PoE firmware changes are NOT automatically performed by the software. You must manually download the new firmware using the "download firmware" CLI command. Until this firmware update is completed, the PoE ports are not powered up. The PoE firmware download may take up to 5 minutes per Alpine FM-32Pi module. It is also subject to failure. Check switch log messages to ensure the firmware change was successful. If unsuccessful repeat the firmware download. Refer to PD3-26645139 in "Clarifications and Known Behaviors" on page 57.*

Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until the firmware update is completed, the PoE ports are not powered up. Refer to "Upgrading PoE Firmware on an Alpine Switch with a PoE Module" on page 47.

## Upgrading Switches to ExtremeWare 7.3

To install ExtremeWare 7.3, you must:

1. Save the configuration to a TFTP server.
2. Upgrade the BootROM to Version 8.2 as described on page 43.
3. Upgrade to ExtremeWare 6.1.9 as described on page 43.
4. Upgrade to ExtremeWare 6.2.2b56 as described on page 44.
5. Upgrade to ExtremeWare 7.3 as described on page 44.
6. Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79 as described on page 45.
7. Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later as described on page 46.
8. Upgrade ATM, MPLS, ARM, or PoS modules as described on page 46.
9. Upgrade the PoE firmware, if required, on the Alpine switch as described on page 47.

If you have already installed ExtremeWare 6.1.9 through ExtremeWare 6.2.2b43, you can skip step 3. If you have already installed ExtremeWare 6.2.2b56 through ExtremeWare 7.0.1, you can skip steps 3 and 4.

**NOTE**

*If you are also upgrading your BlackDiamond to MSM-3's, see the* MSM-3 Upgrade Note *included with your MSM-3.*

**NOTE**

*The Alpine 3802 requires a different upgrade procedure, described on page 47.*

### Save the Current Configuration

Before upgrading ExtremeWare, save your configuration using the following steps. This preserves the ability to downgrade should it become necessary.

1. If you are using the Network Login campus mode:
   a. Disable Network Login using the `disable netlogin` command to prevent users from re-authenticating during the backup process.
   b. Use the `clear netlogin state port` command on all Network Login user ports, causing all Network Login users to be unauthenticated and all client ports to move back to their respective unauthenticated VLAN configuration.
   c. Use the `show netlogin` and `show vlan` commands to verify that all Network Login ports are in the unauthenticated state and the client ports are members of their respective unauthenticated VLANs.
2. If you are using ACLs and the CPU DoS protect feature, ensure that the CPU DoS protect filter precedence follows the rules described in "CPU DoS Protect and ACL Precedence" on page 94. If there is a precedence conflict, CPU DoS protect is not enabled.
3. Save the current configuration in both the primary and secondary configuration spaces using the `save configuration primary` and `save configuration secondary` commands.
4. Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use configuration primary` commands.
5. Verify that all of the above procedures were completed successfully with the `show switch` command.
6. Upload the configuration to a TFTP server for safekeeping using the `upload configuration` command.

### Upgrade the BootROM to Version 8.2

Before you upgrade ExtremeWare, upgrade to BootROM 8.2 (BootROM 8.2 is compatible with all ExtremeWare versions back to ExtremeWare 6.1.9):

1. Download the BootROM using the `download bootrom [<host_name> | <ip_addr>] <ngboot82.bin_name>` command.
2. Reboot the switch using the `reboot` command.

### Upgrade to ExtremeWare 6.1.9

If you are running ExtremeWare 6.1.8 (or earlier), upgrade to ExtremeWare 6.1.9:

1. TFTP download ExtremeWare 6.1.9 to the primary image space using the `download image primary` command.

**CAUTION**

*If you do not upgrade to ExtremeWare 6.1.9 before downloading ExtremeWare 6.2.2, the ExtremeWare 6.2.2 download will fail, and the following message will be printed from the system:*

```
ERROR: File too large
```

2. Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 Check the log for configuration errors. Manually enter configurations that did not load.

5 If you configured Random Early Drop Probability in ExtremeWare 6.1.8 (or earlier), re-configure the Random Early Drop Probability using the `configure red drop-probability` command.

6 Save the configuration to the primary space.

## Upgrade to ExtremeWare 6.2.2b56

If you are running ExtremeWare 6.1.9 to ExtremeWare 6.2.2b43, upgrade to ExtremeWare 6.2.2b56 (you can substitute ExtremeWare 6.2.2 builds 68, 108, 124, 134, and 156 for build 56):

1 TFTP download ExtremeWare 6.2.2b56 to the primary image space using the `download image primary` command.

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

**NOTE**

*ExtremeWare 6.2.2b56 (and later) stores 75 static log entries. Previous versions stored 100 entries. To accommodate the new entry limit, ExtremeWare 6.2.2b56 clears the static log after your first reboot. To preserve your static log entries, use the* `show log` *command and save the output.*

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 TFTP download the saved configuration, and answer `y` at the prompt to reboot the switch.

5 Check the log for configuration errors. Manually enter configurations that did not load.

6 Save the configuration.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

**NOTE**

*After upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.2, the IGMP snooping leave time-out value will be changed from 10 seconds to 0. This results in an IGMP snooping membership entry being removed immediately when an IGMP leave is received from a host.*

*This is good for an environment where only one host is connected. Use the* `configure igmp snooping leave-timeout` *command to change the leave time-out value back to 10 seconds.*

## Upgrade to ExtremeWare 7.3

If you are running any software image from ExtremeWare 6.2.2b56 to ExtremeWare 7.2.0 (or later), upgrade to ExtremeWare 7.3:

**NOTE**

*If you are upgrading a chassis with MSM64i's to MSM-3's, see the MSM-3 Upgrade Note included with your MSM-3.*

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Clear your switch using the `unconfigure switch all` command, and enter `y` at the prompt to reboot the switch. If you started the upgrade process with ExtremeWare 6.2.2b56 or later, you can skip this step.

3 TFTP download ExtremeWare 7.3 to the primary image space using the `download image primary` command.

4 Reboot the switch using the `reboot` command.

**NOTE**

*If you have Hitless Failover enabled on your MSM-3, you can use the hitless upgrade procedure.*

5 Verify that the correct ExtremeWare version is loaded on the switch using the `show switch` command.

6 TFTP download the configuration you saved in Step 1, and enter `y` at the prompt to reboot the switch.

**NOTE**

*If you are using EAPS and are upgrading from a version prior to ExtremeWare 6.2.2b134 or from ExtremeWare 7.0, the default failtimer expiry action changes to sending an alert. This keeps your ring from failing over when there is no break in the ring, such as in the event of a broadcast storm, busy CPU, or misconfigured control VLAN. To change the failtimer expiry action to opening the secondary port, especially if your EAPS traffic flows through switches that do not support EAPS, use the configure eaps failtime expiry-action command.*

7 Check the log for configuration errors. Manually enter configurations that did not load.

8 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

9 If you are upgrading a BlackDiamond switch, synchronize the BootROM, image, and configuration across all installed MSM modules using the `synchronize` command. This command reboots the synchronized modules.

You can ignore any diagnostics failure messages generated by the synchronization.

10 Reboot the switch using the `reboot` command.

11 If you are using the Network Login campus mode:

**a** Manually enable Network Login using the `enable netlogin [web-based | dot1x]` command.

**b** Verify that users are able to authenticate and successfully access network resources.

### Upgrade T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79

If you are using a T1, E1, or T3 module with an ExtremeWare release prior to 6.1.8b79 or a BootROM prior to 2.8, upgrade the module to ExtremeWare 7.3:

1 TFTP download ExtremeWare 6.1.8b79 for the module using the `download image slot primary` command.

**NOTE**

*T1, E1, and T3 modules must be using ExtremeWare 6.1.8b79 and BootROM 2.8 before upgrading to ExtremeWare 7.3.*

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

**NOTE**

*If you are upgrading multiple modules, skip step 3 until you have upgraded every module, then reboot the switch instead of rebooting each slot.*

4 Verify that the correct ExtremeWare is loaded using the `show version` command. You should see output similar to the following:

```
BootROM: 251.251
Image: WM4T1 Version 6.1.8 (Build 79)
```

If you see a version other than Build 79, repeat steps 1 - 4.

5 Download the BootROM using the `download bootrom slot` command.

6 Reboot the module using the `reboot slot` command.

**NOTE**

*If you are upgrading multiple modules, skip step 6, upgrade every module, then reboot the switch.*

7 Download the latest ExtremeWare to the primary image space.

8 Reboot the module using the `reboot slot` command.

### Upgrade T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later

If you are using a T1, E1, or T3 module with ExtremeWare 6.1.8b79 (or later) and BootROM 2.8 (or later), upgrade the module to ExtremeWare 7.3:

1 TFTP download the latest ExtremeWare for the module using the `download image slot primary` command.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

### Upgrade ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 7.3

If you are using an ATM, MPLS, ARM, or PoS module with a previous ExtremeWare release or a BootROM prior to 1.18, upgrade the module to ExtremeWare 7.3:

1 Upgrade your switch to ExtremeWare 7.3 by following the upgrade instructions “Upgrading Switches to ExtremeWare 7.3” on page 42. When your switch is successfully booted on ExtremeWare 7.3.0 continue with step #2.

2 TFTP download ExtremeWare 7.3 for the module using the download image slot primary command.

3 Configure the module to use the primary image with the use image primary slot command.

4 Reboot the module using the reboot slot command.

**NOTE**

*If you are upgrading multiple modules, skip step 4 until you have upgraded every module, then reboot the switch instead of rebooting each slot.*

5 Verify that the correct ExtremeWare is loaded using the show version command.

6 Download the BootROM using the download bootrom slot command.

7 Reboot the module using the `reboot slot` command.

**NOTE**

*If you are upgrading multiple modules, skip step 7, upgrade every module, then reboot the switch.*

8 Verify the slot is operational using the `show slot <#>` command.

### Upgrading PoE Firmware on an Alpine Switch with a PoE Module

If you are using an Alpine switch with a PoE module, upgrade the PoE firmware. A version of PoE firmware is built into ExtremeWare to allow easy replacement if necessary. If the current micro controller firmware becomes corrupted, or requires an upgrade, ExtremeWare logs a message in the syslog prompting for a firmware upgrade.

**WARNING!**

*Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until this firmware update is completed, the PoE ports are not powered up.*

1 Use the following command to download the firmware to the selected slot:

```
download firmware slot <slot_number>
```

2 Verify that the PoE firmware loaded correctly using the `show inline-power stats <slot number>` command.

If the upgrade is not successful, perform the upgrade procedure again.

## Upgrading an Alpine 3802 to ExtremeWare 7.3

To upgrade an Alpine 3802 to ExtremeWare 7.3:

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Upgrade to BootROM 8.2 using the `download bootrom` command.

3 Reboot the switch using the `reboot` command.

4 If you are using an image prior to ExtremeWare 6.1.8b79, TFTP download ExtremeWare 6.1.8w3.0.1 b79 to the primary image space using the `download image primary` command.

5 Verify that the correct BootROM and ExtremeWare versions are loaded on the switch using the `show switch` and `show version` commands.

6 Answer `y` at the prompt to reboot the switch.

7 TFTP download ExtremeWare 7.0.0b46 to the primary image space using the `download image primary` command.

8 Reboot the switch using the `reboot` command.

9 TFTP download the latest ExtremeWare 7.3 build to the primary image space using the `download image primary` command.

10 Reboot the switch using the `reboot` command.

11 TFTP download the configuration you saved in Step 1, and enter `y` to reboot the switch.

12 Check the log for configuration errors. Manually enter configurations that did not load.

13 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

# Downgrading Switches

Assuming that the previous configuration is in the secondary configuration space and the previous image is in the secondary image space:

1 If you saved an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, configure the switch to use that configuration with the `use configuration secondary` command.

If you did not save an earlier configuration, re-configure the switch or download a configuration at the end of this process.

2 If you did not save the earlier ExtremeWare image in the secondary image space, download the image using the `download image secondary` command.

**NOTE**

*If you downgrade to an ExtremeWare version that does not support software signatures (ExtremeWare 6.2.2b56 or later supports software signatures), you must follow the upgrade procedures in the preceding sections to get back to ExtremeWare 7.3. You cannot switch between primary and secondary images on the switch unless they both support software signatures.*

3 Use the image in the secondary image space with the `use image secondary` command.

4 Verify that the above procedures were completed successfully with the `show switch` command.

5 Downgrade to the appropriate BootROM version. The `show version` command displays the BootROM version as "Unknown" when the BootROM is downgraded.

6 Reboot the switch.

**NOTE**

*When downgrading to a previous version of ExtremeWare, ensure that the switch configuration matches that version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported. You will get a warning message from the system when attempting to do so.*

7 If you did not save an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, re-configure the switch or download a configuration.

# 3 Supported Limits

This chapter summarizes the supported limits in ExtremeWare 7.3.

## Supported Limits

The table below summarizes tested metrics for a variety of features. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeWare 7.3 Software User Guide*.

**Table 23:** Supported limits

| Metric | Description | Limit |
|---|---|---|
| Access List rules | Maximum number of Access Lists (best case). | 5120 |
| Access List rules—BlackDiamond 6816 | Maximum number of BlackDiamond 6816 Access Lists (best case). | 3500 |
| Access List rules—Summit | Maximum number of Access Lists in which all rules utilize all available options (worst case). | 255 |
| Access List rules—Alpine | Maximum number of Access Lists in which all rules utilize all available options (worst case). | 255 |
| Access List rules—BlackDiamond | Maximum number of Access Lists in which all rules utilize all available options (worst case). | 255 per I/O module |
| Access Profiles | Maximum number of access profiles per switch. | 128 |
| Access Profile entries | Maximum number of access profile entries per switch. | 256 |
| Application Examination rules | Maximum number of Application Examination rules. | 1000 |
| Application Examination rules/port | Maximum number of Application Examination rules per port. | 60 |
| BGP—Peer Groups | Maximum number of BGP peer groups per switch. | 16 |
| BGP—peers | Maximum number of BGP peers per switch. | 200 |
| BGP—routes, MSM-3 | Maximum number of routes received and contained in the BGP route table (best case). | 835,000 |
| BGP—routes, MSM64i | Maximum number of routes received and contained in the BGP route table (best case). | 300,500 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| BGP—routes, Alpine | Maximum number of routes received and contained in the BGP route table (best case). | 335,000 |
| BGP—routes, Summit7i | Maximum number of routes received and contained in the BGP route table (best case). | 410,000 |
| BGP—routes, Summit48i | Maximum number of routes received and contained in the BGP route table (best case). | 100,000 |
| BGP—routes, Summit5i | Maximum number of routes received and contained in the BGP route table (best case). | 80,800 |
| BGP—NLRI filters | Maximum number of NLRI filters per switch. | 128 |
| BGP—NLRI filer add entries | Maximum number of NLRI add entries per switch. | 256 |
| BGP—AS-Path filters | Maximum number of AS-Path filters per switch. | 128 |
| BGP—AS-Path filter add entries | Maximum number of AS-Path filter add entries per switch. | 256 |
| BGP—network statements | Maximum number of network statements per switch. | 256 |
| BGP—aggregate addresses | Maximum number of aggregate routes that can be originated per switch. | 256 |
| Jumbo Frame size | Maximum size supported for Jumbo frames, including the CRC. | 9216 |
| EAPS—Domains/switch | Maximum number of EAPS domains. | 64 |
| EAPS—Domains/ring | Maximum number of EAPS domains if no switch in the ring is connected to another ring. | 64 |
| EAPS—VLAN links | Maximum number of Control or Protected VLANs per EAPS domain. | 4093 |
| EAPS—Bridge links | Maximum number of EAPS bridge links per switch. | 8192 |
| EAPS—Bridge links | Maximum number of EAPS bridge links on switches with 256MB memory. | 8192 |
| EAPS—Bridge links | Maximum number of EAPS bridge links on switches with 128MB memory. | 4096 |
| EAPS—Master nodes | Number of Master nodes per EAPS domain. | 1 |
| EAPS—Switches | Maximum number of EAPS switches per ring. | No limit |
| EMISTP & PVST+ — maximum domains, Summit | Maximum number of EMISTP and PVST+ domains. | 128 |
| EMISTP & PVST+ — maximum domains, Alpine | Maximum number of EMISTP and PVST+ domains. | 256 |
| EMISTP & PVST+ — maximum domains, BlackDiamond | Maximum number of EMISTP and PVST+ domains. | 512 |
| EMISTP & PVST+ — maximum ports | Maximum number of EMISTP and PVST+ ports. | 3840 |
| EMISTP & PVST+ — maximum domains per port, Summit | Maximum number of EMISTP and PVST+ domains that can be configured per port. | 128 |
| EMISTP & PVST+ — maximum domains per port, Alpine | Maximum number of EMISTP and PVST+ domains that can be configured per port. | 256 |
| EMISTP & PVST+ — maximum domains per port, BlackDiamond | Maximum number of EMISTP and PVST+ domains that can be configured per port. | 512 |
| ESRP—maximum domains | Maximum number of ESRP domains for a single switch. | 64 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| ESRP—maximum instances | Maximum number of ESRP supported VLANs for a single switch. | 64 |
| ESRP—maximum ESRP groups | Maximum number of ESRP groups within a broadcast domain. | 4 |
| ESRP—maximum ESRP groups with bi-directional rate shaping | Maximum number of ESRP groups within a broadcast domain when bi-directional rate shaping is enabled. | 3 |
| ESRP—maximum VLANs in a single ESRP domain – Summit, Alpine | Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain. | 256 recommended; 3000 max |
| ESRP—number of VLANs in a single ESRP domain, BlackDiamond | Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain. | 1024 recommended; 3000 max |
| ESRP—Route-track entries, Summit, Alpine, BlackDiamond | Maximum number of routes that can be tracked for each ESRP domain. | 4 |
| ESRP—maximum VLAN tracks | Maximum numbers of VLAN tracks per VLAN. | 1 |
| FDB—maximum ports for permanent entries | Maximum number of ports supported for permanent FDB entries. | 2000 |
| FDB—maximum L2/L3 entries – BlackDiamond, Summit5i, Summit7i, Alpine 3804, Alpine 3808 | Maximum number of MAC addresses/IP host routes for the MSM64i, Summit5i, Summit7i, Alpine 3804, and Alpine 3808. | 262,144 |
| FDB—maximum L2/L3 entries – Summit1i, Summit48i, Summit48si, Alpine 3802 | Maximum number of MAC addresses/IP host routes for the Summit1i, Summit48i, Summit48si, and Alpine 3802. | 131,072 |
| Flow Redirection—maximum redirection rules | Maximum number of rules that can point to the same or separate groups of web cache servers. | 64 (8 servers is the maximum) |
| Flow Redirection—maximum enumeration mode entries | Maximum number of active entries for enumeration mode rules. For example, one /16 rule can take all of the available entries. | 64,000 |
| Flow Redirection—maximum subnet mode entries | Maximum number of active entries for subnet mode rules. Each mask can have 1 entry. | 64 |
| IP ARP entries | Maximum number of IPARP entries. | 20,480 |
| IP ARP Static entries | Maximum number of permanent IP static ARP entries supported. | 512 |
| IP ARP Static Proxy entries | Maximum number of permanent IP ARP proxy entries. | 512 |
| IP Route Sharing Entries (ECMP)—static or OSPF | Maximum number of static or OSPF routes used in route sharing calculations. | 12 |
| IP Route Sharing Entries (ECMP)—IS-IS | Maximum number of IS-IS routes used in route sharing calculations. | 8 |
| IP Router interfaces | Maximum number of VLANs performing IP routing - excludes SubVLANs. | 512 |
| IP Static Routes | Maximum number of permanent IP routes. | 1024 |
| IPX Static Routes and Services (RIP and SAP) | Maximum number of static IPX RIP route and IPX SAP entries. | 64 for each |
| IPX dynamic routes and services | Maximum recommended number of dynamically learned IPX RIP routes and SAP entries. | 2000 for each |
| IPX Router interfaces | Maximum number of IPX router interfaces. | 256 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| IPX Access control lists | Maximum number of Access Lists in which all rules utilize all available options. | worst case: 255 |
| IS-IS—maximum routing interfaces | Maximum IS-IS routing interfaces. | 255 |
| IS-IS—maximum routes | Maximum IS-IS routes. | 25,000 |
| IS-IS—maximum adjacencies | Maximum IS-IS adjacencies per routing interface. | 64 |
| IS-IS—maximum domain summary addresses | Maximum IS-IS domain summary addresses. | 32 |
| IS-IS—maximum redistributed routes, regular metric | Maximum IS-IS redistributed routes using the regular metric. | 20,000 |
| IS-IS—maximum redistributed routes, wide metric | Maximum IS-IS redistributed routes using the wide metric. | 30,000 |
| IS-IS—maximum redistributed routes, both metrics | Maximum IS-IS redistributed routes using both metrics. | 10,000 |
| Logged Messages | Maximum number of messages logged locally on the system. | 20,000 |
| MAC-based VLANs—MAC addresses | Maximum number of MAC addresses that can be downloaded to the switch when using MAC-based VLANs. | 7000 |
| MAC-based security | Maximum number of MAC-based security policies. | 1024 |
| Mirroring—mirrored ports | Maximum number of ports that can be mirrored to the mirror port. | 8 |
| Mirroring—number of VLANs | Maximum number of VLANs that can be mirrored to the mirror port. | 8 |
| NAT—maximum connections | Maximum number of simultaneous connections per switch. | 256,000 |
| NAT—maximum rules | Maximum number of rules per switch. | 2048 |
| NAT—maximum VLANs | Maximum number of inside or outside VLANs per switch. | The switch's limit |
| NetFlow—Filters | Maximum number of NetFlow filters in a switch. | 128 |
| NetFlow—Groups | Maximum number of NetFlow groups. | 32 |
| NetFlow—Hosts | Maximum number of NetFlow hosts. | 8/group |
| Network Login—Maximum clients | Maximum number of Network Login clients per switch. | 1024 |
| Network Login—802.1x | Maximum recommended Session-Timeout value returned by RADIUS server. | 7200 seconds |
| OSPF areas | As an ABR, how many OSPF areas are supported within the same switch. | 8 |
| OSPF external routes—BlackDiamond, Summit7i, Alpine | Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain. | 100,000 |
| OSPF intra-area routes—BlackDiamond, Summit7i, Alpine | Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain. | 8800 |
| OSPF inter-area routes—BlackDiamond, Summit7i, Alpine | Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain. | 16,000 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| OSPF external routes—Summit1i, Summit5i, Summit48i, Summit48si | Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain. | 27,000 |
| OSPF intra-area routes—Summit1i, Summit5i, Summit48i, Summit48si | Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain. | 2000 |
| OSPF inter-area routes—Summit1i, Summit5i, Summit48i, Summit48si | Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain. | 8000 |
| OSPF routers in a single area | Recommended maximum number of routers in a single OSPF area. | 200 |
| OSPF interfaces on a single router | Recommended maximum number of OSPF routed interfaces on a switch. | 384 |
| OSPF virtual links | Maximum number of OSPF virtual links supported. | 32 |
| OSPF adjacencies—Summit1i, Summit5i, Summit48i, Summit48si | Maximum number of OSPF adjacencies on a switch with 128 MB memory. | 150 |
| OSPF adjacencies—Summit7i, Alpine, BlackDiamond | Maximum number of OSPF adjacencies on a switch with 256 MB memory. | 225 |
| RIP-learned routes | Maximum number of RIP routes supported without aggregation. | 8000 |
| RIP interfaces on a single router | Recommended maximum number of RIP routed interfaces on a switch. | 384 |
| Route Maps | Maximum number of route maps supported on a switch. | 128 |
| Route Map Entries | Maximum number of route map entries supported on a switch. | 256 |
| Route Map Statements | Maximum number of route map statements supported on a switch. | 512 |
| SLB—maximum number of simultaneous sessions | For Transparent and Translational and GoGo modes respectively. | 500,000/500,000/ unlimited |
| SLB—maximum number of VIPs | For Transparent and Translational and GoGo modes respectively. | 1000/1000/unlimited |
| SLB—maximum number of Pools | For Transparent and Translational (does not apply to GoGo mode) | 256/256 |
| SLB—maximum number of Nodes per Pool | For Transparent and Translational (does not apply to GoGo mode) | 256/256 |
| SLB—maximum number of physical servers per group | Applies to GoGo mode only; a group shares any number of common VIPs. | 8 |
| SSH2—number of sessions | Maximum number of simultaneous SSH2 sessions. | 8 |
| SNMP—Trap receivers | Maximum number of SNMP trap receiver stations supported. | 16 |
| SNMPv3—Users | Maximum number of SNMPv3 users. | 32 |
| SNMPv3—Groups | Maximum number of SNMPv3 groups. | 64 |
| SNMPv3—Accesses | Maximum number of SNMPv3 accesses. | 128 |
| SNMPv3—MIB-views | Maximum number of SNMPv3 MIB-views. | 128 |
| SNMPv3—Communities | Maximum number of SNMPv3 communities. | 64 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| SNMPv3—Target addresses | Maximum number of SNMPv3 target addresses. | 16 |
| SNMPv3—Target parameters | Maximum number of SNMPv3 target parameters. | 16 |
| SNMPv3—Notifications | Maximum number of SNMPv3 notifications. | 8 |
| SNMPv3—Filter profiles | Maximum number of SNMPv3 notify filter profiles. | 16 |
| SNMPv3—Filters | Maximum number of SNMPv3 notify filters. | 400 |
| Spanning Tree—maximum STPDs, Summit | Maximum number of Spanning Tree Domains. | 128 |
| Spanning Tree—maximum STPDs, Alpine | Maximum number of Spanning Tree Domains. | 256 |
| Spanning Tree—maximum STPDs, BlackDiamond | Maximum number of Spanning Tree Domains. | 512 |
| Spanning Tree—minimum STPDs | Minimum number of Spanning Tree Domains. | 1 |
| Spanning Tree—802.1d domains | Maximum number of 802.1d domains per port. | 1 |
| Spanning Tree—number of ports | Maximum number of ports that can participate in a single Spanning Tree Domain. | 4096 |
| Spanning Tree—minimum number of ports | Minimum number of ports that can participate in a single Spanning Tree Domain. | 1 |
| Spanning Tree—minimum number of domains/port | Minimum number of Spanning Tree Domains that can be configured per port. | 1 for default VLAN, 0 for others |
| Spanning Tree—Spanning Tree modes | Maximum number of Spanning Tree modes per switch. | 2 (dot1d and dot1w) |
| Standard Multinetting—Maximum secondary IP addresses per switch | Maximum secondary IP addresses that can be configured per switch. | 64 |
| Standard Multinetting—Maximum secondary IP addresses per VLAN | Maximum secondary IP addresses that can be configured per VLAN. | 64 |
| Static MAC FDB entries—Summit, Alpine, BlackDiamond | Maximum number of permanent MAC entries configured into the FDB. | 4096 |
| Super-VLAN—number of ports & sub-VLANs | Maximum number of ports and sub-VLANs associated with each super-VLAN. | 2550 |
| Syslog servers | Maximum number of simultaneous syslog servers that are supported. | 4 |
| Telnet—number of sessions | Maximum number of simultaneous Telnet sessions. | 8 |
| UDP profiles | Number of profiles that can be created for UDP forwarding. | 10 |
| UDP profile entries | Number of entries within a single UDP profile. | 16 |
| VLANs—Summit, Alpine | Includes all VLANs plus sub VLANs, super VLANs, etc. | 4095 |
| VLANs—BlackDiamond 6816 fully populated | Includes all VLANs plus sub VLANs, super VLANs, etc. | 681 |
| VLANs—BlackDiamond 6816 with up to 7 I/O modules | Includes all VLANs plus sub VLANs, super VLANs, etc. | 1776 |
| VLANs—BlackDiamond | Includes all VLANs plus sub VLANs, super VLANs, etc. | 4095 |
| VLANs—maximum active protocol-sensitive filters | The number of simultaneously active protocol filters in the switch. | 15 |

**Table 23:** Supported limits (continued)

| Metric | Description | Limit |
|---|---|---|
| VRRP—maximum VRIDs | Maximum number of unique VRID numbers per switch. | 4 |
| VRRP—maximum VRIDs with bi-directional rate shaping | Maximum number of unique VRID numbers per switch when bi-directional rate shaping is enabled. | 3 |
| VRRP—maximum VLANs/switch | Maximum number of VLANs per switch. | 64 |
| VRRP—maximum VRIDs/VLAN | Maximum number of VRIDs per VLAN. | 4 |
| VRRP—maximum ping tracks | Maximum number of ping tracks per VLAN. | 4 |
| VRRP—maximum iproute tracks | Maximum number of iproute tracks per VLAN. | 4 |
| VRRP—maximum VLAN tracks | Maximum number of VLAN tracks per VLAN. | 1 |

# 4 Clarifications, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification, behaviors that might not be intuitive, and issues that have been resolved since the last release. Numbers in parentheses are for internal reference and can be ignored.

This chapter contains the following sections:


- Clarifications and Known Behaviors on page 57
- Issues Resolved in ExtremeWare 7.3.2b3 on page 105
- Issues Resolved in ExtremeWare 7.3.1b3 on page 107
- Issues Resolved in ExtremeWare 7.3.0b49 on page 108
- Issues Resolved in ExtremeWare 7.3.0b44 on page 110


## Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 7.3. For changes made in previous releases, see the release notes specific to the release.

### General

#### optrambusywait Error Message

The switch is generating otpRamBusyWait errors when running multicast or broadcast traffic (PD3-3389453).

#### IP Multicast FDB Entry Incorrect

IP multicast FDB entries are incorrect after transitioning from master to slave with ESRP and load sharing (PD3-23761794).

### LACP Does Not Detect Link Down

If LACP packets are not received on a particular port, then LACP should detect that as a link down situation and remove that port from the aggregation group. This only occurs when auto-negotiation is off on the ports.

**Workaround.** Enable auto-negotiation on both sides of the link.

(PD3-19098058)

### Smart Redundancy

Packet forwarding does not work properly after failing over twice on a Summit 48si switch with smart redundancy enabled.

**Workaround.** Enable smart redundancy.

(PD3-16316575).

### Changing Auto Negotiation

With auto-negotiation disabled on a disable port, the link does not come up once the port is enabled and has changed Auto Neg to ON.

**Workaround.** Change auto-negotiation, disable the port, and enable it again.

(PD3-9556226)

### ARP Response from MPLS to MSM

The ARP responses from the MPLS I/O module to the MSM I/O module might be dropped due to backplane congestion. This method of communication between the two I/O modules does not provide separation between ARP response traffic and other data traffic.

**Workaround.** For the entries showing incomplete ARP, ping the host from the switch. This clears the incomplete entry.

(PD2-244409133)

### HTTPS Access

HTTPS is only available on the Alpine switches (PD3-2489351).

### Unable to Download Image to a Switch with 500 Configured IP VLANs

Reduce the number of configured IP VLANs to 400 on a switch with no management port. This would allow you to download a new software image (PD3-3575589).

### NP API Generates Error Messages When Disabling a Slot Containing an OC3 or OC12 Module

The NP API generates log error messages whenever you disable a slot that contains an OC3 or OC12 module. The same error messages are generated when you hot plug an OC3 and OC12 module. The

`NPAPI can not reboot` error message is continuos, occurring about every 5 (+/-) seconds, and will fill up the log. You will also receive an oobPollTask error message about every 5 minutes (PD2-249436801).

### Cannot Ping localHost Loopback Interface

You cannot ping the localHost loopback interface (PD3-2791311).

### Hot-swapping an MSM3 Causes Invalid MAC Address on Backplane EEPROM

When you hot-swap an MSM-3, the following log message is generated:

```
CRITICAL ERROR: Backplane EEPROM has invalid MAC Address. System halted
```

(PD3-1514691)

### MSM-3 Displays Broken Connection Recovered Message when Hot-swapping and Inserting an MSM64i

If you hot-swap and insert an MSM64i and have an MSM-3 installed, the MSM-3 generates the following log messages:

```
<Crit:SYST> The broken connection between MSM-A mother board port 24 and I/O module
1 port 6 is recovered
```
(PD3-1221174)

### Hot-Swapping an MSM Causes I/O Modules to Reset

Hot-swapping an MSM generates the following log messages:

```
<Info:SYST> cardScan: <msm insert> Attempting to fix card 2 in reset <FFFFFFFF>.
<Info:SYST> cardScan: <msm insert> Attempting to fix card 4 in reset <FFFFFFFF>.
```

In the above message, card 2 and card 4 are not present; all of the other cards are present (PD3-1206991).

### Downloaded Configuration Might Cause Syntax Error With Enable Web Command

A configuration file uploaded to a server, then downloaded to the switch, might cause a syntax error when the switch reboots. The downloaded configuration file caused a syntax error when it reached the entry, "enable web http access-profile none port 80" (PD3-3192200).

### Wireless Error Messages Display During Bootup

If two APs are connected to the switch and are online when the switch is rebooted, the following error messages are displayed during the reboot:

```
Jul 31 07:12:50 SYST: Invalid security profile with index 2
Jul 31 07:12:50 SYST: Port and interface binding not found
Jul 31 07:12:50 SYST: Request for req_type=WI_SECURITY_PROFILE: No such wireless
interface 3:1:1 (index=300101)
Jul 31 07:12:50 SYST: Request for req_type=WI_SECURITY_PROFILE: No such wireless
interface     3:1:2 (index=300102)
```

These messages only occur when no slot information is configured and do not impact switch performance (PD3-3017484).

### show pim snooping Command Shows an Incomplete List of Packets Snooped

The `show pim snooping <vlan>` command shows an incomplete list of the PIM control packets snooped for the specified VLAN if you are sending more than 10 data streams. This is primary seen with (S,G) entries (PD3-2721014).

### MSM-Failover Link-Down Not Working on the Remote Side

The MSM-failover link-down does not bring down the link on the remote side of the switch. It only brings down the link on the fiber ports (PD2-246448118).

### ExtremeWare 7.3 introduces the concept of QoS profiles on a VLAN

QoS profiles refer to the queue configuration of physical ports. The standard way to configure QoS profiles for ports is by using port numbers. If you configure a QoS profile on a VLAN, the QoS profile is applied to all of the ports on the VLAN. However, if the port belongs to multiple VLANs, any QoS profile changes made on the different VLANs affect the same physical port configuration. The QoS profile changes correspond to the last configured value on the port. The configuration can be either directly as a port or because of being a part of a VLAN (PD2-243742697).

### Repeatedly Hot-Swapping the MSM Might Cause Loss of Connectivity

If you remove and re-insert the backup MSM several times in a row (above 5 times), you might temporarily lose connectivity between the MSM and the I/O modules (PD2-231933106).

### Cannot Save or Download a Configuration If a “ghost” Process is Running in the Background

If you issue the `save configuration` command, you might get the following error message:

```
Failed to save config: a save or download is in progress - please try again Later
```

This error message can be generated if you are trying to save or download a configuration while the switch already has a save or download configuration process running in the background. There are instances where the switch appeared to have a “ghost” save or download configuration process running but did not. This error message can be issued if a save or download configuration process was interrupted.

**Workaround.** Reboot the switch. This should clear the ghost processes and allow you to save and download the configuration again (PD2-231288723).

### Creating an ACL with a Filter-Precedence of 11 or 12 Generates a Conflict Error with cpu-dos-protect

When enabling cpu-dos-protect on the switch, a filter-precedence of 10 (default) is used. If you configure another ACL with a filter-precedence of 11 and 12, a conflict error with CPU DOS Protection is generated (PD2-241094151, PD2-241094160).

### Hot-Swapping Modules Might Cause Misleading Error Messages

A module that is receiving broadcast traffic might generate misleading error messages as it is removed. The messages will be similar to the following: `<Erro:Bridge.FrameError> Cannot send packet out.Card=7 not present 04/21/2004 21:15:00.17` (PD2-231933101).

### G12Ti Module Link Detection Fails

Link detection will fail on G12Ti ports set to 100 Mbps full duplex, with autonegotiation set to off, if you do not use the correct cabling. Auto cross detection does not properly detect this condition. As a workaround, use the correct cable (PD2-232279701).

### Autonegotiation Between Fiber Optic Ports is not Possible

A port from a Fast Ethernet switch, when connected to any gigabit port, does not recognize the speed mismatch. The port appears active even though the gigabit port is inactive (PD3-2073971).

### show log Command Memory Error

When running debug-trace for AgentX-APi, the `show log` command output shows an AP failure due to the switch being "out of memory," even though it is not (PD3-2617791).

### unconfigure switch all Command Should Not Restore the Downloaded Configuration

When downloading a new configuration to the switch, you are prompted with the following message:

```
New configuration file has been successfully downloaded to memory.

To make the new configuration effective, the system needs to reboot.

Would you like to reboot the system? (Y/N)
```

If you choose `N`, the new configuration should not take effect. Issuing the unconfigure switch all command should restore the switch to the factory defaults. However, instead of restoring the factory defaults, the switch again applies the previously downloaded configuration (PD3-2536041).

### WLANSYST Output of the show log Command is Not Correct

The output for the `show log` command always shows the WLANSYST message twice. This does not impact switch performance (PD3-2450049).

## System Related – All Systems

### The NVRAM Dirty Bit Being Set from the PoE Code

The NVRAM dirty bit is being set from the PoE code that saves the connection history (PD3-2963230).

### PoE Firmware image Download is not Available in Base Image

The PoE firmware image has been removed from the base image. The current base image will give an error message if it detects a PoE module on an Alpine switch. For the PoE feature to work correctly, use the unified (.xtr) image, not the base (.Bxtr) image (PD3-2011501).

### Autonegotiation Setting Not Preserved on Added and Deleted Loopback Ports

If you add a 10/100 port as a loopback port and delete it, autonegotiation is set to off (PD2-192574401).

### Configure Slot for PoE Before Configuring or Downloading PoE Configuration

You must configure a slot for a PoE module before downloading a PoE configuration. Downloading a PoE configuration to a switch without a PoE module configured generates an error message similar to the following:

```
Error:  slot 8 is not PoE capable!
```

To avoid this, configure the slot for a PoE module before saving the configuration (PD2-209577118).

### The show log Command Truncates Long Commands

If you download a configuration, the output of the `show log` command might not completely display commands longer than 240 characters. This is a display problem; the configuration loads correctly (PD2-171470611).

### The show log Display Truncates Configuration Parsing

If you download a configuration and use the `show log` command to view the parsing of the configuration, the log does not display the entire parsing. This is a display problem; the configuration parses and loads correctly (PD2-171470601).

### Do Not Create Single-Character Names

When you create named components such as VLAN or access group names, do not use single character names. The single character might be interpreted by the switch as a truncated parameter. For example, if you name an SNMPv3 access group "a" and delete that access group using the `configure snmpv3 delete access a` command, the switch might interpret the command as `configure snmpv3 delete access all-non-default` (PD2-152594408).

### Smart Redundancy Enabled in Saved Configuration

Smart redundancy is always enabled in a saved configuration. To work around this, disable smart redundancy after downloading a configuration (PD2-128133503).

### Telnet and the show ports Command

If you telnet to the switch and use the `show ports info detail` command, the line feeds might not be recognized, resulting in output lines overwriting previous lines (PD2-130127501).

### The show configuration Output

After using the `unconfigure switch all` command, the `show configuration` output displays the VLAN *default* without any ports assigned. The ports still belong to the VLAN *default*, as the `show vlan` output correctly displays (PD2-128233941).

### Upgrading to ExtremeWare 7.0 and Bi-Directional Rate Shaping

When you directly upgrade from ExtremeWare 6.2.2 to ExtremeWare 7.0 (or later), bi-directional rate shaping does not work if the loopback ports were in autonegotiation mode. This behavior is not displayed by 10/100Base-T or Gigabit fiber ports. A workaround is to remove and re-add the loopback ports to the VLAN (PD2-107820904).

### Upgrading to ExtremeWare 7.0 and Debug-Trace

When you directly upgrade from ExtremeWare 6.2.2 to ExtremeWare 7.0 (or later), the debug-trace configuration might change. Verify the debug-trace configuration, if any, after upgrading. Use the `show debug-trace` command to display the configuration. You can either re-configure manually, or download the ExtremeWare 6.2.2 configuration instead of doing a direct upgrade (PD2-106733988).

### Upgrading to ExtremeWare 7.0 and OSPF

If you upgrade directly from ExtremeWare 6.2.2 to ExtremeWare 7.0 (or later), the OSPF metric for 10 Gigabit interfaces is incorrect. A workaround is to manually configure the OSPF metrics, or to upload the configuration before upgrading and then download the ExtremeWare 6.2.2 configuration (PD2-108161623).

### Blank Space in show port info detail Command Output

The output of the `show port info detail` command contains several blank pages. The output still contains all of the requested information (PD2-107800978).

### Using an ExtremeWare 7.0 Configuration with an Earlier Image

If you are using an ExtremeWare 7.0 (or later) configuration and attempt to use an earlier image, the switch prompts you for confirmation (because this combination is not recommended). If you answer "`n`" at the prompt, you receive the following error message:

```
Error: bad image.
```

You can safely ignore this message (PD2-110983501).

### Console Response with a Large Number of ARP Entries

Console response is slow when the switch is learning 10,000 or more ARP entries. This does not affect performance. Console response returns to normal when the entries are learned (PD2-104103941).

### The show log chronological Command

When the syslog contains more than 1,000 lines, the `show log chronological` command displays nothing. However, the command `show log` displays correctly (PD2-104062736).

### BOOTP-Dependent Routes in Downloaded Configuration not Created

Static and default routes that depend on a BOOTP IP address/subnet are not created when you download a configuration (PD2-86888351).

### The disable learning Command and Flooding

The disable learning command does not remove the port from the security flood list. Thus, you cannot disable flooding when learning is disabled (PD2-73199618).

### Port Tag Limitation

There is an absolute limit of 3552 port tags available in a system. The usage of these port tags depends on a combination of factors:

- Installed ATM, MPLS, ARM, and PoS modules

- Mirroring
- IPX routing
- Static FDB entries

If the switch reaches the limit of available port tags, the following messages appear in the syslog:

```
<WARN:HW> tNetTask: Reached maximum otp index allocation
<WARN:HW> tBGTask: Reached maximum otp index allocation
```

If this occurs, you must compromise some features (for example, mirroring) in order to expand your use of other functionality. (1-E5U7Y).

### WinSCP2 Not Supported

The application WinSCP2.exe is not supported. Using WinSCP2 does not cause any problems (1-A5C6C).

## BlackDiamond

### Broadcast or Unknown Unicast Packet Sent to Same Ingress Port

Unknown broadcast and unicast packets are being sent to the same ingress port when removing or inserting a MSM B. When you run the `show port stats` command, the transmitted packet counter will show approximately 50-100 packets after the MSM B insert (PD2-244409162).

### ExtremeWare 7.0 (and Later) Does Not Support xmodem

You cannot use xmodem to transfer ExtremeWare 7.0 (or later) to an MSM (PD2-245681101, PD2-137101701).

### Secondary MSM Access Error

The following access error might be logged in the `show diagnostics` command output while the secondary MSM is in the reset state after running the `synchronize` command:

```
07/14/2004 14:51:50.00 <Crit:ENG> ENG: trxdiag: Twister access on MSM-B failed
(tmp=31)
```

This does not affect switch performance and there is no need for any hardware replacement (PD3-1437438, PD3-1437361).

### Loopback Port Must be on Same Module on a BlackDiamond Switch

The loopback port must be on the same module as the rate shaped ports. Though you can configure a loopback port on another module, this is still not a supported configuration. This applies to BlackDiamond switches only (PD2-124299901).

### Two Trap Messages Sent for Hard Reset/Soft Reset on BlackDiamond 6816

When performing a hard reset/soft reset on a BlackDiamond 6816 with SNMP traps configured, two SNMP traps are sent. On the BlackDiamond 6816 this behavior occurs repeatedly with both MSM-A and MSM-B having MSM3s (PD3-1135809).

### Targeted LDP Sessions Become Operational When MPLS is Disabled

Issuing the command, `show mpls ldp`, might display operational targeted LDP sessions, even on switches with MPLS disabled. The TLS tunnel VC state is displayed as "Complete" and the LSP state is displayed as "Down." No traffic traverses the tunnel. There is no workaround (PD2-229043816).

### BGP Fast Fail-over Does Not Work for Change of IP Address

If a BGP session exists with fast-failover enabled and the connection has been established with large keepalive and hold timer values, if you change the IP address, BGP will continue to stay in the established state until the hold timer expires.

**Workaround.** Do not allow IP address changes to be made to the VLAN transmitting BGP traffic (PD2-238197001).

### CMT Group Will Not Forward Traffic Without a Master Slot

When you create a cross-module trunk (CMT) group with the master slot missing or disabled, the group will not forward traffic. A save and reboot will resolve the problem. If a working CMT group already exists, and that group is disabled and re-enabled, the CMT group works correctly (PD2-175975513).

### Connection to G12SXi Might be Lost

If you reboot a BlackDiamond, you might lose the connection between the MSM64i and a G12SXi in slot 4 of a BlackDiamond 6804 or BlackDiamond 6808, or in slot 9 of a BlackDiamond 6816 (PD2-149449300). Messages similar to the following are generated:

```
<CRIT:SYST> [2] The connection between MSM-A mother board and I/O module 4 is broken,
need to fix immediately
<INFO:SYST> Start initializing module in slot 4
<INFO:SYST> Generating default port configuration for slot 4 module oper type G12SXi
config type Unknown
```

To avoid this, install the G12SXi in a different slot, or use an MSM-3. To work around this, reboot the switch again. For more details, see Field Notice FN 0147.

### MPLS and ESRP

When a TLS VC is configured for an ESRP sub VLAN, the TLS VC is not deactivated when ESRP goes into the slave state (PD2-85254107).

### EAPS and Hitless Failover

If you have an EAPS domain with one MSM64i installed in the master switch and two MSM-3s installed in the transit switch, the master switch enters the unknown state when you initiate hitless failover on the transit switch (PD2-219743398).

### Cross-Module Trunking and Hitless Failover

For traffic load-shared across I/O modules, failover is not hitless; traffic loss occurs for approximately four seconds (PD2-186133901).

### Autonegotiation Off Command Accepted on 10 Gigabit Ethernet Modules

Although you cannot disable autonegotiation on the 10 gigabit Ethernet modules, the command to turn off autoneogtiation is accepted and the resulting display shows autonegotiation status as off (PD2-223283401, PD2-232279703).

### Memory Corruption with RRO on PATH Message

When the egressing switch receives an RSVP PATH message with a Record Route Object (RRO) from a directly attached peer with the Session Attributes Flags set to Label Recording Requested, the switch might crash. This can happen when the Session Attribute Flags field indicates Label Recording Requested on a non-Extreme Networks switch (PD2-213821701).

**Workaround.** Disable the Label Recording Request on the non-Extreme Networks MPLS switch and reboot.

### No Longer Display Stale TLS NHLFE Entries

Using an LSP tunnel label that is no longer valid creates stale TLS NHLFE entries that might cause lost date packets. This can be caused by a configuration change, by an LSP going down and back up, or when the label for a tunnel LSP is changed without the LSP going down and back up (PD2-203414601).

**Workaround.** Reboot the slot with the MPLS module.

### MPLS Module Might Not Be Recognized

When you have more than one MPLS module in your chassis and you enable MPLS, one of the modules might not be recognized. If an MPLS module is not recognized, reboot the slot (PD2-199489301).

### LSP NHLFE Not Updated

The values for the LSP NHLFE are not updated in the MPLS module when the downstream label is changed. This might be the result of a change in the TLS's address (PD2-203606001).

**Workaround.** Reboot the slot with the MPLS module.

### Removing Second MPLS Module Causes Traffic to Stop

If you remove an MPLS module from a chassis with more than one MPLS module installed and using a TLS tunnel, traffic stops. To work around this, replace the MPLS module (PD2-199171622).

### Disabling One MSM Might Cause Loss of Throughput

If you disable one MSM in a dual-MSM configuration, you might lose half of the throughput on ARM and MPLS modules (PD2-199171610).

The output of the `show diagnostics backplane utilities` command shows slots with ARM or MPLS modules as having only two backplane links, rather than the normal four backplane links.

### Cannot Delete an LSP Previously Referenced by a TLS Tunnel

You cannot delete an LSP previously referenced by a TLS tunnel. To delete the LSP, first reboot the switch (PD2-222522101).

### EAPS Trap Not Sent if Connection is Through I/O Port

If the EAPS secondary port link is down, the EAPSStateChange trap is not sent to the management station if the connection is through an I/O port that is part of the protected VLAN instead of to the management port. To avoid this, connect the management station through the management port or an I/O port that is not on the protected VLAN (PD2-180185834).

### The card-down Option

In a fully redundant configuration, if you configure the `card-down` option in the `configure sys-health-check` command and checksum errors are detected, the MSM is not taken offline as expected. To work around this, use the `configure sys-health-check auto recovery 3 offline` command (PD2-105991401).

### 10 Gigabit Ethernet and CMT

If you use 10GLRi or XENPAK ports with the address-based or round robin load-sharing algorithms and the master link is lost, FDB entries are not learned (PD2-197753713).

### XENPAK with the BlackDiamond 6816

On a BlackDiamond 6816, if you configure the MSM to keep links up, save the configuration, and reboot the switch, XENPAK links do not come up (PD2-198280301).

### Cross-Module Trunking Not Supported on MSM64i's

If you enable cross-module trunking on a chassis with MSM64i's installed, you receive the following error message:

```
All load share ports must be on the same module
```

Cross-module trunking is not supported with MSM64i's. To enable load sharing across modules, install MSM-3's (PD2-193845958).

### Cross-Module Trunking Module Support

Table 24 lists the modules that support load-sharing across modules.

**Table 24:** Cross-module trunking module support

| Module | CMT Support |
|---|---|
| G8Xi | Yes |
| G8Ti | Yes |
| G12SXi | Yes |
| G16X[3] | Yes |
| G24T[3] | Yes |
| F32Fi | Yes |

**Table 24:** Cross-module trunking module support (continued)

| Module | CMT Support |
|---|---|
| F48Ti | Yes |
| F96Ti | Yes |
| WDMi | No |
| 10GLRi | Yes |
| 10GX3 | Yes |
| MPLS | No |
| ARM | No |
| P3cMi | No |
| P3cSi | No |
| P12cMi | No |
| P12cSi | No |
| A3cMi | No |
| A3cSi | No |

Cross module trunking is not supported on WDMi modules (PD2-176314520).

### Master Slot Must Be Active for CMT

The slot with the master load-sharing port must be populated and active when you configure a cross-module load-sharing group. If the master slot is unavailable at configuration, cross-module load-sharing traffic is not forwarded (PD2-175825901, PD2-175854401).

### MSM-3 Log Might Be Out of Chronological Order

Log events are stored independently on the master and slave MSM-3. Thus, a failover might cause the log to appear out of chronological order, or missing information. Concatenating the logs provides all log information (PD2-172852704).

### Source Addresses Might Age Out of FDB

If a MAC source address is exclusively sourced on a slave CMT slot, such as with a port-based algorithm, the FDB entry might be aged out. To avoid this, use address-based load sharing on the neighbor switch (PD2-170942776).

### Do Not Use Static FDB Entries with CMT

Do not use static FDB entries with cross-module trunking. If the CMT master fails, static FDB entries are not transferred to the group members (PD2-170942732, PD2-170942701).

### Saving Health Check Configuration After Failure Causes Console Crash

If an MSM fails a system health check with packet memory errors and is taken offline, the slave becomes the master, but you cannot save the configuration. To avoid this, clear the diagnostics, upload the configuration, and reboot the switch before saving (PD2-171914501).

### Diagnostics on MSM-3 with Hitless Failover Causes Failover and Spurious Message

Running diagnostics on the master MSM-3 with hitless failover enabled causes the MSM-3 to fail over to the slave and log a hardware failure message. You can safely ignore this message (PD2-168317013).

### Do Not Configure a Port-Based Backplane Algorithm When CMT is Enabled

Do not configure a port-based backplane policy when CMT is enabled. It might cause all egress ports on a given slot to be skipped. To work around this problem, configure an address-based backplane policy. In a similar manner, if a port-based algorithm is selected for the trunk, some egress ports might be skipped. To change the load share policy of a trunk, disable sharing for the port and enable sharing with an address-based policy, then reboot the switch (PD2-165883601).

### Cross-Module Trunking and ACLs

Flooding on a CMT trunk cannot initially be blocked by ACLs. After the remote end responds with a PDU, the destination address is learned via source address learning. Once the address is learned, packets are blocked in hardware by an ACL (PD2-153404501, PD2-115139620, PD2-130299801, PD2-130299807).

### 4,000 VLANs on a BlackDiamond

If you configure more than 4,000 VLANs, EDP might crash, causing ESRP to fail (PD2-153821210).

### E1 Module and the restart port Command

After you use the `restart port` command, E1 modules occasionally fail to establish a physical link (PD2-85857901).

### PPP Links Through E1 modules

PPP links through the E1 module are not always re-established after a reboot. To re-establish the PPP link, use the `restart ports` command (PD2-109252301).

### Slot Failure Messages During a Broadcast Storm

If you have more than 15 Gigabit Ethernet links between two chassis, all in the same VLAN and generating a broadcast storm, the system health check records slot failures in the log. When the broadcast storm stops, the log messages also stop (PD2-117946811).

### No Image Information Reported to SNMP with One MSM

If you only install an MSM in slot B of a BlackDiamond 6804, BlackDiamond 6808, or BlackDiamond 6816, no primary or secondary image information is reported to your SNMP NMS (PD2-129612901).

### BlackDiamond 6816 MSM C and D Diagnostics Messages not in Syslog

If you run diagnostics on an MSM in slot C or D of a BlackDiamond 6816, messages are not recorded in the syslog. To view the diagnostics messages, use the `show diagnostics` command (PD2-118049501).

### Disabling CLI Paging from the Slave MSM64i

Enabling or disabling CLI paging from the slave MSM64i has no affect on the master MSM64i paging configuration (PD2-104377501).

### The unconfig switch all Command

If you use the `unconfig switch all` command and immediately use the `config default vlan delete port all` command, the switch reboots (PD2-105474401). To avoid this situation, after you unconfigure the switch, wait for the switch to completely reboot before you delete the ports.

### BlackDiamond 6816 MIB Value for Input Power Voltage

On the BlackDiamond 6816, the extremeInputPowerVoltage attribute in extremeSytemCommonInfo is shown as "0" and the extremePowerSupplyInputVoltage in the extremePowerSupplyTable is shown as "unknown." These values cannot be obtained from the switch (1-841J1).

## Alpine

### Mirroring Failure on an Alpine 3808 with GM4x Module After a Save and Reboot

Port mirroring might fail on the Alpine 3808 with a Gigabit Ethernet, 4-port, GBIC module after saving and rebooting the switch. As a workaround, disable and enable the mirroring port after rebooting the switch (PD3-1025737).

### With IE5.0 Vista Page is not Accessible Through HTTPS

Using IE5.0, you cannot access the Vista page through HTTPS. However, you can access the Vista page through HTTPS using IE5.5+ (PD3-2738891).

### Autonegotiation on VDSL Ports Set Incorrect Speed

A VDSL port configured to autonegotiate sets the speed to 100 Mbps when connected to a 100 Mbps port (PD2-209953030). The maximum speed for the VDSL port is 10 Mbps. As a workaround, configure autonegotiation off, and set the speed to 10 Mbps, full duplex. For example, to configure port 3:1, use the following command:

```
configure port 3:1 auto off speed 10 duplex full
```

### VDSL Ports do not Support Jumbo Frames

Do not enable jumbo frames on VDSL ports. Jumbo frames are not supported on VDSL ports (PD2-208090059).

### New Accounts with WAN Module Installed are pppuser

If you have a WAN module installed and you create a user account, the account is automatically created as pppuser (PD2-197374626).

### Limited Commands Mode

When in limited commands mode, the slot status LED remains orange, though the link is taken down (PD2-99107226).

### VDSL Modules in a Half-Duplex Link

A VDSL CPE operating in a half-duplex link can lock up when used with a hub and running wire-rate randomized traffic. This is a hardware limitation. A restart of the VDSL port will recover, but if the traffic continues at wire-rate and is randomized, then the problem will reoccur (PD2-71538118).

## Summit

### Spurious Summit48si Power Supply Messages

When a Summit48si powers up, some power supplies might generate error messages similar to the following:

```
<INFO:SYST> PSU-A output failure recovered.
<INFO:SYST> PSU-A powered on.
<INFO:SYST> PSU-A powered off.
```

You can safely ignore these messages (PD2-208576301).

### Output of the show log Command

The most common reason for transceiver diagnostics failure is heat. Thus the `show log` output displays the TRXDIAG tag in the temperature log message (PD2-147462529).

### The unconfigure switch all Command Clears the Default VLAN from s0

After you reset the switch to the factory defaults using the `unconfigure switch all` command, s0 does not contain the default VLAN. To add the default VLAN to s0, delete then add all ports in the default VLAN (PD2-143709201).

### Health Check Error Messages

Error messages from the system health check display the incorrect location (PD2-110132842).

### Summit48i Redundant PHY

When the primary port of a redundant pair is disabled and the link removed, the LED for that port continues to flash indicating it has a link and is disabled (9239).

### Summit48i Single Fiber Signal Loss

The Summit48i is currently not able to detect a single fiber strand signal loss due to the hardware based Auto Negotiation parameters (10995).

### SNMP Results for Power Sources

The inputPower MIB is unable to differentiate between 110 VAC and 220 VAC input on the Summit series switches when accessing this MIB attribute through SNMP (10870).

### Summit48si MIB value for Input Power Voltage

On the Summit48si, the extremeInputPowerVoltage attribute in extremeSytemCommonInfo is shown as "0" and the extremePowerSupplyInputVoltage in the extremePowerSupplyTable is shown as "unknown." These values cannot be obtained from the switch (1-841J1).

## PoE

### PoE Firmware Update Can Occasionally Fail

Image upgrades or downgrades that involve a PoE firmware change on an Alpine FM-32Pi PoE module may fail during the firmware update or change. The following console message indicates that the update or change was not successful.

```
PoE system on slot 1 not operational
Slot 1 PoE firmware update failed
```

If this message is displayed you will be required to reboot the switch before the PoE firmware change takes effect. PoE functionality does not operate until the firmware change is successful. The following message indicates that the firmware change was successful.

```
PoE system on slot 1 initialized
Slot 1 PoE firmware update completed (0)
```

(PD3-26645139)

## Command Line Interface (CLI)

### IGMP Snooping Not Disabled on MAC VLAN

IGMP snooping is enabled on a MAC VLAN Discover even after issuing the disable IGMP snooping command and save/reboot the switch.

**Workaround.** After rebooting the switch, disable IGMP snooping again.

(PD3-19498525)

### Mirroring Cannot be Disabled

Mirroring cannot be disabled until all mirroring ports are deleted (PD2-244886705).

### Console Does Not Wait for User Input

The console is not waiting for a response after issuing the prompt `Continue? (yes or no) <<<`. When you press the ENTER key, the key strokes being sent are CR+LF. With a console connection, the switch interprets this as though you pressed the ENTER key twice. This problem does not occur if you are using a Management port connection.

**Workarounds.**

- Connect through the Management port.
- Change your terminal setting to Ctrl+M instead of CR+LF (TELNET new line) if using PuTTY version 0.54.

- Use Tera Term. When using Tera Term, CR is sent by default instead of CR+LF.

(PD2-247002201)

### Command Does Not Function

The functionality associated with the command `configure wireless ports x:x interface x client-scan keep-ies [on|off]` is not implemented. The command exists on the switch, but is not functional (PD3-3004440).

### show fdb vpls Command Does Not Accurately Show the Correct Total of FDB Entries

The `show fdb vpls` command does not show the correct total of FDB entries running on the switch (PD3-2780831).

### clear counters Command Does Not Clear Number Transmitted in a MPLS Health Check

The `clear counters` command does not clear the number of VPLSPINGS sent by the switch (PD3-2570481).

### show fdb port Command Does Not Reflect Correct FDB Data for that Port

The `show fdb portlist` command shows the same total as the `show fdb` command for the entire switch. For example, if you issue the `show fdb po 1:1` command, the output should show two MAC addresses whereas a total of 55 is shown (PD3-1857861).

### Maximum Number of ESRP Groups Supported in the ESRP MIB is Incorrect

The maximum number of supported ESRP Group and ESRP Neighbor Group is from 0 to 31, not 1 to 65535, as stated in the ESRP MIB table (PD2-244686417).

### Not All configure debug-trace Options Are Displayed

The following `configure debug-trace` command options are available but are not displayed:

- ap-scan
- client-diag
- mac-radius
- wpa
- iapp

(PD3-2179879)

### SNMP Trap Commands Not Supported

The `disable snmp trap port-up-down port mgmt` and `enable snmp trap port-up-down port mgmt` commands are not supported by the CLI. To enable or disable SNMP port-up-down traps on the management port, use SNMP (PD2-162482918).

### The show ports mgmt info Output Missing Flags

The output of the `show ports mgmt info` command does not display the flags (PD2-156475701).

### Press [Return] Key Twice With enable temperature-log Command

You must press the [Return] key twice when entering the `enable temperature-log` command. If you only press the [Return] key once, the system does not display the asterisk indicating a configuration change. The log is correctly enabled by pressing the [Return] key once (PD2-152215201).

### User Sessions Cannot Enable CLI Paging

You cannot enable CLI paging when logged in to a user account. It is enabled by default (PD2-145565305).

## Switching and VLANs

### Renew/Refresh Required After Each Logout To Get IP Address

A DHCP enabled VLAN port might assign the same IP address to different clients. If you do not perform a release/renew after each logout, other clients might not be able to get an assigned IP address from the internal DHCP server (PD3-3255805).

### Packets Sent to VRRP-MAC That Do Not Belong to the VRID of the VLAN are also Being Accepted

Packets that are sent to VRRP-MAC that do not belong to the VRID of the VLAN are also being accepted. This occurs when the same port is added to more than one VRRP VLAN as tagged (PD2-244356901).

### The show iproute Output

The output of the `show iproute` command now displays only the first eight characters of the VLAN name (PD2-128392829).

### MAC-Based VLAN Configuration Not Saved

If you configure and enable a MAC-based VLAN, save the configuration, and reboot the switch, the configuration is lost (PD2-224261163).

### Load Share Group Might Fail Back to Group with Fewer Ports When Using Software Redundant Ports

If you have a primary load share group that fails over to the redundant load share group, and you remove and reinsert the I/O module that contains the primary load share group, traffic fails back to the primary load share group even though the primary load share group has fewer active ports. However, if another port in the primary group fails, traffic correctly fails over to the redundant load share group.

For example, ports 1:1-1:5 are the primary load share group and ports 2:10-2:15 are the redundant load share group. If you remove the cables from ports 1:1-1:3, the load share group fails over to ports 2:10-2:15. If you remove and reinsert the I/O module installed in slot 1 and do not attach the cables to ports 1:1-1:3, the load share group fails back to the primary load share group. If you then remove the cable from port 1:4, traffic fails over to the redundant load share group (PD2-223253601, PD2-225707301, PD2-246246401, PD2-246246404).

### Saving ip-mtu Settings

Dynamic TLS (Martini TLS) checks the MTU received from its peer in order for TLS to come to the established state. It compares against the egress VLAN's IP-MTU. If the egress VLAN does not have an IP address defined, any non-default ip-mtu setting will not be saved through a switch reboot (PD2-64084527).

### VLAN priority and STP, EDP

STP and EDP (thus ESRP and EAPS) do not transmit packets in the queue specified by the VLAN priority (1-5HOZ9).

### Default Routes or Static Routes

If you define a default or static route, and then delete the VLAN on the subnet associated with the default route, the default route entry remains although it is invalid. You must manually delete the configured route.

If you define multiple default routes, the one with the lowest metric is used. If there are multiple routes with the same lowest metric, the switch picks one of the routes.

### Configuring a Protocol Filter with 'ffff'

Creating a protocol filter with LLC of value 0xffff and assigning it to a VLAN will not work, and should not be attempted. Doing so will assign all traffic to the VLANs containing that filter and will prevent VLANs with no protocol filter to function properly. If configured and saved, you must issue an `unconfigure switch all` to restore normal operation (2644, 4935).

### Deleting Protocols from a VLAN

Adding a protocol to a VLAN might cause an EPC if the protocol was added to the VLAN, deleted from the VLAN, recreated by the user, and re-added to the VLAN (6128).

### MAC-Based VLANs and DHCP Relay

MAC based VLAN configurations should not be used in conjunction with DHCP. Currently, a host which enters a MAC-based VLAN will not be able to use DHCP to obtain an IP address.

### VLAN to VLAN Access Profiles

VLAN to VLAN access profiles are no longer supported on the BlackDiamond switch in ExtremeWare 6.0 or higher (7022).

## FDB

### FDB Entries Disappear Before Aging Timeout

If you `configure fdb agingtime` to 100,000 seconds, the FDB entries disappear before the 100,000 seconds. The values disappear around 200+ seconds (PD2-248579601).

### Cannot Add FDB Entry for Management VLAN

You cannot add an FDB entry for the management VLAN (PD2-156475718)

### MAC Security

The source FDB address configuration will not discard ICMP packets (16340).

### FDB Aging Timer

In ExtremeWare 6.2.0, the default value of the FDB aging timer was set to 1800 seconds on a newly configured ExtremeWare 6.2.0 switch. In ExtremeWare 6.2.1 the default value has been changed back to 300 seconds. However, when upgrading from ExtremeWare 6.2.0 to ExtremeWare 6.2.1, the default value will remain 1800 seconds. For upgrades from ExtremeWare 6.1.9 (or earlier) the default value will remain 300 seconds. The FDB aging time can still be set to all previous values (1-85QD3).

### Configure Less Than 400 Ports in a VLAN

If you use the `clear slot` command (which flushes the FDB) when there are 256,000 or more FDB entries, the watchdog timer can cause the switch to reboot. To avoid this, configure less than 400 ports in a VLAN (PD2-90223209).

## Load Sharing

### Removing Modules During CMT Testing Causes Loss of Traffic

When you perform the CMT trunk up/down tests and remove the modules and re-insert them, the switch receives 50% less traffic. As a workaround, after you re-insert the modules and notice a 50% loss of traffic, remove the ports and re-insert them (PD3-2162531).

### Backplane Algorithm Not Working Properly When Changing the Algorithm from Address-Based to Port-Based

When the backplane algorithm is changed from address-based to port-based the backplane still behaves as an address-based algorithm, causing the traffic to appear on all ports instead of one port. As a workaround, save and reboot the switch after changing the backplane algorithm (PD2-238168901).

### Autonegotiation

Load sharing ports must be configured with autonegotiation set to on. Load sharing ports will not transmit traffic correctly using any other setting (PD2-64617405).

### Round Robin Load Sharing

If a port in a round robin load share group is removed, the traffic that was being transmitted on that link will be distributed on only 1 of the other active load share links in the round robin group. The traffic is not distributed evenly between the remaining ports (6977).

### Port Based Load Sharing on Summit7i

Port-based load sharing on the Summit7i requires ingress ports to be on the same side of the switch (ports 1 - 4, 9 - 12, 17 - 20, and 25 - 28 on the left, ports 5 - 8, 13 - 16, and 21 - 24 on the right) as the 8 ports in the load share group for all ports in the load share group to transmit/receive traffic (6975).

### Alpine and Cross Module Load Sharing

The I/O module configured to contain the "master" port must be physically present in a cross-module load sharing group for the system to pass traffic (8589, PD2-119098401).

### Load Sharing and Specific Ports in a Load Share Group

Due to the load sharing algorithm used for round robin load sharing, when using 3, 5, 6 or 7 ports in a load share group packet loss will be observed when sending wire-speed traffic across the load share group. This occurs because some ports will be selected to transmit more packets than other ports resulting in bandwidth over-subscription and subsequent packet loss. This only occurs with round-robin load sharing configurations (10311).

### Disabling Load Sharing if the Master is Down Generates Error

If the load sharing master link goes down, and you disable load sharing, the switch generates a ptag error message (PD2-129379272).

## Mirroring

### Port Mirroring Does Not Work on Rate Shaping Loopback Port

You cannot use port mirroring on a port you have configured as a loopback port for ingress rate shaping (PD2-243424420).

### Delete Mirroring Filters Before Disabling Mirroring

You must delete all mirroring filters before you disable mirroring on the switch. If you attempt to disable mirroring before deleting the mirroring filters, an error message similar to the following appears: `ERROR: Delete mirrored port(s) before disabling mirroring`.

If you see this message, use the `configure mirroring delete` command to delete the mirroring filters followed by the disable mirroring command to disable mirroring (PD2-246368703).

### Port from Deleted VLAN Mirrors When Added to New VLAN on Alpine Switch

On an Alpine switch, if you configure a VLAN port for mirroring, delete the VLAN, and then add the original port to a new VLAN, it is still configured for mirroring (PD3-1757651).

### Do Not Configure Port Mirroring While Port is Down

If you reconfigure port mirroring while the physical port is down, switched traffic that crosses a routing boundary is duplicated (PD2-147476551).

# ELSM

### Spurious Error Message with ELSM

Disabling or enabling ELSM or the ELSM auto-restart port feature might generate an error message similar to the following:

```
hfoCliEvent: Command does not support Hitless Failover
```

You can safely ignore these messages (PD2-182478105).

# Spanning Tree

### Adding or Deleting a Port from a VLAN Flushes FDB on All STP Protected VLANs

Adding or deleting a port from a VLAN flushes FDB on all STP protected VLANs, which causes the flow redirect rules with ping tracking configured to also go down (PD2-245992601).

### show vlan STP Output is not Correct

The output for the `show vlan` command does not mark the flag as "T" (member of the STP domain) when the VLAN has no ports associated with it. Because the VLAN has no associated ports, it is not shown as part of the STP domain (PD2-246881901).

### STP Topology Change in One STP Domain (S1) Flushes FDB in Other STP Domain (S2)

When two STP instances (S1 and S2) in dot1w mode share the same physical ports, that is, the physical port is part of both domains, then a topology change in one STP domain (S1) will flush the FDB learned in the other STP domains (PD2-145439733).

### STP CPU Utility Usage Increases and Drops Ping Packets

The STP task CPU utility increases up to 20% and drops ping packets when adding/deleting a port from the VLAN. Disabling or enabling ports, or adding a tagged port to the VLAN does not affect switch performance. A workaround is to enable STP on ports that have STP disabled (PD2-236187221, PD2-239254001).

### Disabling ignore-bpdu Adds CPU MAC Entry to FDB

If you disable ignore-bpdu, an entry for the CPU MAC is added to the FDB for the VLAN (PD2-225957431).

### Enabling STP on MAC-based VLANs Might Cause Connectivity Loss

On a BlackDiamond, if you enable STP on a MAC-based VLAN, you might experience a loss of connectivity (PD2-223958706).

### Incorrect Log Message

If you reboot after enabling STP and VLANs, the device might log the following incorrect message:

```
<STP.OutBPDU.Drop> Port=8:2: Illegal message age (65517)
```

This is a display issue only; functionality is not affected (PD2-208909326).

### RSTP Does Not Detect Topology Change

If a physical link transitions from down to up when the ports are configured with point-to-point links and 802.1w, RSTP does not detect a topology change (PD2-197365089).

### Disabling STP Might Display Topology Change

When you disable STP, the output of the `show stpd` command displays a topology change. If there was not actually a topology change, you can safely ignore this indicator (PD2-165211765).

### FDB Not Flushed After Link Failure with RSTP

When using RSTP, the FDB is not flushed when recovering from a link failure. This is the expected behavior (PD2-143730501).

### Do Not Configure All Ports in s0

With all ports on several FM-32 modules in s0 and more than 256,000 FDB entries continuously learning, deleting a range of ports from a VLAN, adding the same range to another VLAN, deleting them from that VLAN, then adding them back to the first VLAN can cause a watchdog reboot. Do not configure all ports in s0 (PD2-118450167).

### Error Messages with Topology Changes

If you have STP domains configured on a switch and add active ports to the domain, bringing the links up and down might generate error messages similar to the following (PD2-159834201):

```
<Erro:STP.OutBPDU.Drop> Port=4:13: Illegal message age (21)
```

### Large STPD Configuration Download Might Reboot Switch

If you download a configuration with more than 70 STP domains, and each domain has more than 120 VLANs, the switch might reboot. To avoid this, disable the system watchdog timer, download the configuration, and enable the timer (PD2-136044092).

### A Large STP Configuration with 10 Link Transitions

If you have more than 120 802.1w STPDs with more than 2,000 total VLANs, a link failover might form a loop. The loop might last as long as 40 seconds, depending on the number of VLANs configured (PD2-135691018).

### Configure Fewer than 4,000 VLANs in an STPD

If you add more than 4,000 VLANs to an STP domain, the switch might run out of memory (PD2-135842818).

### Output of show stpName port detail Command in Hex Format

The output of the `show stpName port detail` command displays the `PortID` in hex format instead of decimal format. If you do not specify the `detail` parameter, the output correctly displays in decimal format (PD2-136044001).

### If You Delete a Port from the STPD, You Cannot Add It Through a VLAN

If you delete a port from the STPD, then add a VLAN containing that port to the STPD, the deleted port is not added. To work around this, add the port back to the STPD (PD2-144382901).

### The unconfigure stp Command Does Not Clear All Configurations

The `unconfigure stpd` command does not clear the tag, VLAN, operational mode, rapid root failover, port mode, or port link-type. To clear these configurations, use the `delete stpd` command (PD2-137310575).

### Enabling ignore-bpdu or ignore-stp

If you enable ignore-bpdu or ignore-stp on a VLAN and then enable STP, the switch still participates in STP election. To work around this, reboot the switch (PD2-140533593).

### Configuring a VLAN from Vista

If you create an STPD using ExtremeWare 6.1.9 (or earlier), add a VLAN, save the configuration, upgrade to ExtremeWare 6.2.2b68 (or later), and save the configuration, you receive the following error message when you try to modify the VLAN from Vista:

```
ERROR: Cannot assign bridge to stpd! HINT: If a port is part of multiple vlans, the
vlans must be in the same Spanning Tree domain.
```

To work around this problem, make configuration changes from the CLI (PD2-118450190).

### STP and VLAN Tagging

VLAN tagging is not supported with 802.1d Spanning Tree (STP) BPDUs. Therefore, all BPDUs in a 802.1d STP domain are untagged. However, Extreme Multiple Instance Spanning Tree (EMISTP) and Per-VLAN Spanning Tree (PVST+) do support VLAN tagging of BPDUs.

### EMISTP and Ingress Rate Shaping

If a loop exists in your network, but STP is not enabled and Ingress Rate Shaping is, the switches appear to hang and are rebooted by the watch-dog timer. A similar situation exists if a loop is covered by STP on both sides and is disabled on one side; normally the other switch immediately blocks the right port(s), but when Ingress Rate Shaping is present, both switches appear to hang and are rebooted by the watch-dog timer (1-5E9R1).

### Upgrading From an ExtremeWare 6.1.9 (or earlier) Configuration

After downloading an ExtremeWare 6.1.9 (or earlier) configuration to an ExtremeWare 6.2.0 (or later) image, a port belonging to a non-default VLAN generates the “Stpd s0, Port 1:1 does not exist” error message because that VLAN does not belong to domain s0 by default (1-BMP5D).

## ESRP

### ESRP Master Does Not Change to the Neutral State

The ESRP Master might not change to the neutral state on the super-VLAN, even though there are no active ports on any of the sub-VLANs.

**Workaround.** Disable the ESRP on the VLAN and enable it again (PD2-251147301).

### The disable slot all Command Generates EDP Errors

If you have ESRP enabled, the `disable slot all` command generates EDP errors. You can safely ignore the error messages (PD2-166105101).

### Large Configurations Might Lock Console when Enabling and Disabling s0

If you have more than 60 STP domains with more than 200 tagged VLANs between them and more than 6 ports in each, and you enable then immediately disable s0, the console might freeze for up to a minute. Larger networks cause the console to remain locked for longer periods. The switch is still operating, and the console unlocks after the processing finishes. To work around this, either wait before disabling s0, or wait until the console unlocks (PD2-159834277, PD2-151426418).

### ESRP and Protocol-Based VLANs

ESRP-aware switches cannot connect to an ESRP switch through a port configured for a protocol-sensitive VLAN using untagged traffic (PD2-99007701).

### ESRP and Load Sharing

If you enable load sharing on ports that belong to more than 200 VLANs, the switch reboots. To avoid this, first enable load sharing, then add the ports to the VLANs (PD2-99259801).

### Hot-Swapping a Module with 5,000 ACLs

Hot-swapping a module on a switch that has 5,000 or more ACLs configured can cause an ESRP state change (PD2-107800998, PD2-103938301). To avoid the state change, configure the neighbor timeout value to 12 seconds.

### Traffic Convergence Time

Traffic convergence after a link failure can take as long as 5 seconds with 2,000 VLANs and 256,000 FDB entries. This delay can cause ESRP state changes as traffic converges (PD2-89915300).

### ESRP PDUs on Ports

ESRP PDUs received on ports that do not belong to any VLAN are processed as valid ESRP PDUs and can trigger state changes (PD2-89481346). To avoid this, assign all ports to valid VLANs with matching tags.

## ELRP

### ELRP and Ingress Rate Shaping

Do not use ingress rate shaping on an ELRP-enabled VLAN (PD2-133066184).

# VRRP

### Proxy ARP Replies on VRRP Enabled VLANs Are Incorrect

When sending out proxy ARP replies on a VRRP enabled VLAN, the sender MAC address in the ARP Reply contains “System MAC” instead of “VRRP MAC” (PD3-1275521).

### Backup Transition Creates Duplicate Packets

A VRRP transition from backup to master might cause duplicate data packets to be transmitted for a short period of time. The packets are dropped, so no action is required (PD2-129379226).

# QoS

### DiffServ QoS Priorities Apply Per Block

On a Summit 200-48 switch, QoS/ACL rules are configured on a 24-port block basis(1-24, 25-48). The priorities configured on one port block do not apply to another port block. If the traffic ingresses from one port block, use the egress on the same port block (PD3-24338771).

### QoS Profiles Applied to Non-Master Ports in Load Sharing Groups

Although QoS profiles should only be applied to the master port in a load sharing group, the CLI does not enforce this behavior. When a QoS profile is applied to a non-master port, the CLI accepts the command, issues no error, but does not apply the profile (PD2-243742691).

### QoS Profile Statistics Are Not Shown for Non-master Ports in a Loadshared/CMT Group

When a QoS Profile is applied to traffic being transmitted through the trunk ports (CMT), the QoS profile statistics for some ports is 0, even though the port statistics show that the traffic is being sent through the same ports (PD2-235114601).

### The qosprofile Accepts a Value Greater than 100%

The `maxbw` parameter in the `configure qosprofile` command incorrectly accepts values greater than 100%; however, the maximum bandwidth is still 100% (PD2-123662004).

### Re-Ordering Access List Precedence Numbers

When you add a new ACL rule with a precedence number, the switch re-orders existing rules with lower precedence numbers to make room for the new rule. If, during this re-ordering, two rules have a precedence number difference greater than one, the switch generates an error message similar to the following:

```
<WARN:KERN> Access rule does not exist
```

You can safely ignore this error message (1-FAO8M).

### Access List FDB Entries not Cleaned Up

If you delete an access list with the “f” flag (flow rule), the associated FDB entries might not be cleared (PD2-110082518).

### Access Lists Using the IP Deny Any Rule

When using an access control list with an IP deny any rule, all ICMP traffic will be blocked within a VLAN (Layer 2). If using an access list with an IP deny any rule across VLANs (Layer 3), ICMP traffic will not be blocked.

### Access Lists and IP Fragmentation

When using IP fragmentation, since the TCP header is treated as data and only the IP header information is being replicated in each packet, access-lists that apply to that flow will not apply as the TCP/USP port information is not included after the first fragment (for subsequent fragments).

### QoS Configuration Bandwidth Parameters

Minimum and maximum percentage parameters for a specific port on the default VLAN will not be saved across reboots. The configuration change will be applied when configured. This issue only occurs on the BlackDiamond (15500).

### Creating Access Lists from Multiple Sessions

When creating or modifying access control lists, please ensure that no other administrator sessions are attempting to create or modify the system access control lists simultaneously. This might result in data corruption (1-579HD).

### 5,120 Access Lists and SNMP

Although you can configure up to 5,120 ACLs, SNMP only recognizes 1,280. Deleting an ACL that is not recognized by SNMP generates the following error (PD2-64880917):

```
<WARN:SNMP> SNMP IPQOS Could not find entry instance 5083 to delete
```

### Monitoring QoS and the show port qos Command

When monitoring QoS, do not use the `show port qos` and `enable qosmonitor` commands on the same port at the same time. These commands in conjunction lock the console session. However, the syslog does capture the output (PD2-64202681, PD2-80836531).

## MPLS

### Cannot Delete TLS VLAN After Deleting TLS Tunnel When MPLS is Disabled

You cannot delete a TLS VLAN after you delete a TLS tunnel when MPLS is disabled. To delete the TLS VLAN, enable MPLS or reboot the system (PD3-2553271).

### IP Interface of Local End-point VLAN for TLS Tunnel or VPLS Can be Modified

When you configure a VLAN with loopback-mode and IP forwarding enabled, and an IP address, a TLS tunnel or VPLS is configured using this VLAN as the local end-point. You can disable IP forwarding when either the TLS tunnel or VPLS is using the VLAN as a local end-point. The IP address of the VLAN can be changed or unconfigured when a VPLS is using the VLAN as the local end-point, but not the TLS tunnel (PD2-243426413).

### Clear Counters Command Does Not Clear RSVP LSP Count

The clear counters command does not clear the RSVP LSP count (PD3-3250311).

### Targeted LDP Sessions Become Operational When MPLS is Disabled

Issuing the command, `show mpls ldp`, might display operational targeted LDP sessions, even to switches with MPLS disabled. The TLS tunnel VC state is displayed as "Complete" and the LSP state is displayed as "Down." No traffic traverses the tunnel. There is no workaround (PD2-229043816).

### Targeted LDP Sessions do not Come Up When OSPF is Disabled and Router ID is Automatic

When router ID is automatic, and OSPF is disabled, the router ID is 0.0.0.0. When a TLS tunnel or VPLS is created in this state, the source address is copied from the router ID. A workaround is to manually set the router ID or enable OSPF first (PD2-218047403).

## Bi-Directional Rate Shaping

### Secondary MAC Used for Rate Shaping Not Released

When you have added a rate-shaping port to a VLAN and then to a load-sharing group, that port is removed from the VLAN. In this situation, the secondary MAC address used for rate limiting is not released (PD2-249582310)

### Aggregate-Bandwidth Granularity Correction

The granularity for the aggregate-bandwidth must be closely aligned with the configured values (PD2-249336801).

**Table 25:** Bandwidth Configuration for Hierarchical Rate Shaping

| | Suggested Bandwidth Configuration | |
|---|---|---|
| **Requited Bandwidth** | **Fixed Frame Size** | **Random Frame Size** |
| 3 | — | 3 |
| 5 | — | 6 |
| 8 | — | 8 |
| 10 | 15 | 10 |
| 15 | 20 | 15 |
| 20 | 25* | 20 |
| 25 | 25 | 25 |
| 30 | 30* | 30* |
| 35 | 30 | 35 |
| 40 | 40 | 40* |
| 45 | 45 | 40 |
| 50 | 50* | 50 |
| 55 | 55* | 50 |

**Table 25:** Bandwidth Configuration for Hierarchical Rate Shaping

| | Suggested Bandwidth Configuration | |
|---|---|---|
| **Requited Bandwidth** | **Fixed Frame Size** | **Random Frame Size** |
| 60 | 65 | 60 |
| 65 | 65 | 65 |
| 70 | 70* | 70* |
| 75 | 75 | 70 |
| 80 | 80 | 80 |
| 85 | 85 | 80* |
| 90 | 90 | 85* |
| 95 | 95 | 95 |
| 100 | 100 | 100 |

**NOTE**

*Numbers marked with an asterisk (*) have appreciable discrepancy on the higher side. For example, if the port is configured for 70% bandwidth, 72% bandwidth might be seen.*

### SecureMac Flags Not Shown

SecureMac flags are not shown on FDB entries of rate shaped ports (PD2-171300406).

### Locking and Unlocking Learning

If you configure a rate shaping port to lock learning and unlock learning, the loopback FDB is not flushed. This causes traffic destined for the port to be flooded. You must manually flush the FDB using the `clear fdb` command (PD2-124568416).

### 1000Base-T Ports as Loopback Ports

If the loopback port for bi-directional rate shaping configurations is configured on 1000Base-T ports, the speed of that port cannot be changed from 1000 Mbps to 100 Mbps as the bandwidth settings will not be accurate when configured in 100 Mbps mode.

## EAPS

### Cannot Delete a VLAN from EAPS Domain

You cannot delete a VLAN from an EAPS domain in certain scenarios if warning messages are ignored (PD3-21774911).

### Configuring Cross Module Trunking Causes EAPS Failure

When configuring cross module trunking, if you connect a slave port, the transit switch does not forward the EAPS hello packets and the EAPS ring is in the failed state (PD2-238232230).

### Shared-Port Link ID Limits

When you configure a shared-port link ID, the CLI does not enforce a limit. However, if you input a value greater than 65535, the value is chopped to be within the range 1 - 65535 (PD2-243424458).

### EAPS Performance Statistics

Table 26 lists the EAPS performance statistics for a single EAPS domain with the default filter.

**Table 26:** EAPS performance statistics with the default filter

| Protected VLANs | Link Down Convergence Upstream (ms) | Link Down Convergence Downstream (ms) | Link Up Convergence Upstream (ms) | Link Up Convergence Downstream (ms) |
|---|---|---|---|---|
| 1 | 106 | 101 | 100 | 99 |
| 500 | 260 | 220 | 170 | 130 |
| 1,000 | 310 | 220 | 170 | 227 |
| 4,000 | 534 | 533 | 675 | 900 |

Table 27 lists the EAPS performance statistics for a single EAPS domain with no filters.

**Table 27:** EAPS performance statistics with no filters

| Protected VLANs | Link Down Convergence Upstream (ms) | Link Down Convergence Downstream (ms) | Link Up Convergence Upstream (ms) | Link Up Convergence Downstream (ms) |
|---|---|---|---|---|
| 1 | 1.9 | 1.8 | 1 | 1 |
| 500 | 54 | 54 | 70 | 100 |
| 1,000 | 106 | 106 | 170 | 226 |
| 4,000 | 415 | 415 | 675 | 900 |

Table 28 lists the EAPS performance statistics for a single EAPS domain with a single protected VLAN and varying FDB sizes.

**Table 28:** EAPS performance statistics with varying FDB sizes

| FDB Entries | Link Down Convergence Upstream (ms) | Link Down Convergence Downstream (ms) | Link Up Convergence Upstream (ms) | Link Up Convergence Downstream (ms) |
|---|---|---|---|---|
| 2,000 | 2.4 | 3.2 | 1.1 | 1.2 |
| 10,000 | 2.5 | 3.5 | 1.3 | 1.4 |
| 50,000 | 4 | 5 | 2.8 | 3 |
| 100,000 | 5 | 6 | 4 | 4 |

### ESRP and EAPS Secondary Port

Configuring ESRP Host Attach on an EAPS secondary port causes a broadcast storm (1-B1O4L).

### Incorrect show vlan Output

The `show vlan` output incorrectly lists the EAPS secondary port as active with an asterisk (*). The number of active ports is correctly displayed (PD2-59142420).

# IP Unicast Routing

### Reset the FDB Aging Timer

When you disable multinetting, you must reset the FDB aging timer to 300 seconds using the `configure fdb agingtime` command (PD2-160697401).

### No Static ARP Entries

The use of Static ARP entries associated with superVLANs or sub-VLANs is not supported in this release (5106).

### ARP Entry Age

The age of ARP entries changes to a large value when system time is changed (1-E7FIV).

### Multinetting and the Show VLAN Stats Command

The `show vlan stats <vlan_name>` command is not supported on multinetted VLANs (12196).

### Multinetting and VRRP

Multinetting is not supported with VRRP (1-9YG1B).

# IPv4 Routing

### PIM CRP Timer Error

If you configure the PIM CRP timer to a high value and then reconfigure the timer to a lower value, the lower value is not accepted. The switch continues to use the original higher value to send out the advertisements. As a workaround, delete the existing CRP and add it again, or add another CRP (PD2-249465903).

# RIP Routing

### Access Profile Does Not Block Default Route from Being Advertised, in case of RIP Export Filter

If you configure two switches for RIP configuration and set one switch to export a default route into RIP, and configure an export filter on the VLAN that is advertising the RIP updates, the access-profile does not block the default route from being advertised (PD3-19630284).

### Problems with Default Route Origination Addition and Purging

Default routes are not being sent and withdrawn using trigger update messages. When you issue the `disable rip` command, the default route is removed from the peer routing table after the route timeout duration (PD2-243713601).

### RIPv1 Learned Routes Might Not Be Purged Immediately

When a RIPv1 learned route has a matching subnet on one of the learning router's own interfaces, and when the subnet mask of that particular interface is modified, the RIP routes with both the subnet ranges are advertised to it neighboring RIPv2 peer. This can create blackholes in the network for the RIP route timeout duration (PD3-2535701).

### RIPv2 Authentication

The authentication feature of RIPv2 is not supported.

### RIP in Conjunction with other Routing Protocols

It is recommended that RIP be enabled only on routers running with less than 10,000 routes from other routing protocols, such as BGP or OSPF.

## OSPF

### Duplicate IP Addresses Causing OSPF Route Flapping

In a duplicate IP address scenario (IP address configured on a VLAN (with no ports), and also added to OSPF), the route to IP address keeps flapping if the VLAN interface comes up before the neighboring LSA update (PD3-21817289).

### OSPF Originate Default Cost Can Be Set Incorrectly

When configuring OSPF Originate Default, an incorrect cost of 0 (zero) is accepted. If you configure the OSPF Originate Default cost to 0 (zero) the default route will not propagate (PD2-213413326).

### LSA Batch Interval Not Supported

The LSA batch interval feature is not currently supported. Though you can configure the feature, (PD2-222030701).

### Static Route with Switch's Address as Gateway Not Advertised

If you configure a static route with the switch's IP address as the gateway, that route is not advertised. To avoid this, do not use the switch's IP address as the gateway (PD2-222030705).

### AS-external LSAs Might Not Be Regenerated

AS-external LSAs are not regenerated after an active LSA is removed or a neighbor goes down (PD2-149426154).

### Error Message Not Generated

If you configure a low ase-limit with a lot of type-5 LSAs, enabling OSPF causes a database overflow state before OSPF adjacency is built. This should generate a critical error message, but does not (PD2-148164866).

### Disable OSPF Before Adding or Removing External Area Filters

If you configure an OSPF area external filter on an ABR, and the filter is set to exclude routes that have already been learned, an OSPF failure occurs. A workaround is to disable OSPF before adding or removing OSPF external area filters (PD2-105170634).

## IS-IS

### Unicast Packets Considered Broadcast

Unicast packets are occasionally considered broadcast packets and dropped (PD2-142499344).

## BGP

### improper Handling of EXT Length Bit Flag in BGP AS_PATH Attribute

The extended length bit flag in the as-path attribute is not reset when the as-path attribute length is less than 256 (PD3-23295761).

### A Session Down Due to Max Prefix Limit Will Not Re-establish

BGP peering Session that goes down as a result of exceeding the peer maximum prefix limit restriction without the Hold timeout option, will fail to re-establish itself, unless that BGP peer session is disabled and enabled again (PD3-3333831).

### Large Number of Access Profiles and a Peer Reset

You can add a maximum of 10 BGP community numbers in inbound and/or outbound route updates using access-profiles and/or route-maps. If you add more communities, BGP might crash (PD2-160136950).

### Default Route Might Not Be Deleted

If you have the export of static BGP routes enabled, the IP route table has a default static route and BGP is redistributing the default route using the `configure bgp add network` command, then after you delete the default route from BGP using the `configure bgp delete network` command, the default BGP route is not withdrawn from the neighbor's table (PD2-159150038).

### BGP Aggregation with a Maximum Prefix of 300,000

Disabling BGP, configuring the maximum prefix to 300,000 or more, enabling BGP aggregation, configuring some aggregate routes, and enabling BGP generates error messages similar to the following (PD2-147347223):

```
<Erro:BGP.Misc.DelAggrtNetErr> Count lost sync for Net 202.7.243.0 Mask 255.255.255.0
```

### Redistributing BGP Routes to OSPF

Redistributing 70,000 or more BGP routes into OSPF depletes the system resources and the switch might run out of memory, causing task exceptions. Do not redistribute 70,000 or more BGP routes into OSPF (PD2-74932501).

# IP Multicast Routing

### System Fails After Receiving PIM Bootstrap Packet

The system fails after receiving a PIM bootstrap packet with a length of more than 1700 bytes, which is more than the link MTU size (PD3-22561301.

### PIM SM Switch Reboot will not Re-establish the Existing Multicast Traffic Present Before Reboot

If multicast traffic is flowing through a switch configured for PIM SM, and that switch is rebooted, the steam will be dropped (PD3-3359901).

### PIM DM Switch Reboot Might Delay Re-establishment of Traffic

If multicast traffic is flowing through a switch configured for PIM DM, and that switch reboots, it might take a long time to re-establish the traffic (PD3-3031243).

### (S,G) Packets are Sent to CPU When Route to Source is Lost in Last Hop Router

If a PIM SM enabled router looses the route towards the Source (S) but has interested receivers (*,G), all the multicast packets are directed to the CPU (PD3-2423281).

### The unconfigure igmp Command Does Not Unconfigure All Parameters

The `unconfigure igmp` command does not set the `forward-mcrouter-only` or `flood-list` parameters to the default values (PD2-141266115).

### If PIM-Snooping is Enabled on Current Traffic, All (S,G) Entries Will be Marked as Invalid

If traffic is present before PIM-Snooping is enabled, or the PIM-Snooping switch reboots as traffic is present, all (S,G) entries will be marked as invalid. If PIM-Snooping was enabled before the traffic is received, the entries are marked correctly (PD2-229351706).

### Enable or Disable IGMP Snooping on a Sub-VLAN

To disable or enable IGMP snooping on a sub-VLAN, delete the sub-VLAN from the super-VLAN, change the IGMP snooping status, and add the sub-VLAN to the super-VLAN (PD2-136478101).

### Do Not Disable IGMP Snooping with Static Snooping Entries

If you disable IGMP snooping on a VLAN, the configured static IGMP snooping entries do not reply to the IGMP querier, while real hosts attached to the VLAN will (PD2-158477713).

### (S,G) Entry Not Created if RP is Rebooted

An (S,G) entry is not created if the RP is rebooted (1-F4YIP).

### Cisco Interoperation

For proper Cisco interoperation, use Cisco IOS version 11.3 or later, which supports PIM 2.0. Cisco customer support also recommends using PIM in favor of DVMRP whenever possible on Cisco routers (4669).

### Traffic Rate Exceeding Last Hop Threshold

When the traffic rate exceeds the configured last hop threshold, the last hop does not initialize; but if the sending traffic rate is set to 50 Kbps, it switches to STP correctly (1-57NMY).

## Network Login

### Multiple Supplicants

When multiple supplicants are used, if one of the supplicants is authenticated, then traffic from all other supplicants is allowed without authentication. This is not observed in the Alpine platform (PD2-237953257).

### TCP SYN and TCP ACK Not Working Correctly

TCP/HTTP connection is accepted after the user has logged out in Campus mode Network Login (PD3-21387942).

## Security

### Enhanced DoS Protection Feature Limitation

With enhanced-dos protection enabled, for each packet received on an interface for the first time, a node is inserted in the enhanced DoS FDB cache with ipDest address as the key. If another packet is received on a different interface but with the same destination IP, the received packet is dropped. Eventually, the OSPF packets also get dropped because of the destination IP address. This does not allow the switch to respond to simultaneous ping sessions (PD3-23075521).

## Changing VLAN and Wireless Port IP Causes RADIUS Proxy Failure

Authentication failures occur when you change the VLAN and wireless port IP resulting in a RADIUS proxy failure (PD3-7388921, PD3-6751371).

### Cannot Apply a New Port after Creating a Trusted MAC Entry on a VLAN

When creating a trusted-mac-address on a VLAN and omitting the port option, the trusted MAC is applied to all ports in the entire VLAN. However, the trusted MAC does not apply the newly added port. You must manually apply trusted MAC to the newly added port (PD3-3625781).

### Unconfiguring a Slot will not Remove the Ports from Network Login and Network Login Cannot be Disabled

When unconfiguring a slot with Network Login enabled on a port, Network Login is not removed. However, the ports are removed from the default VLAN, and Network Login cannot be disabled on the

port because the VLAN does not contain the port. As a workaround, to disable Network Login on the port, add the port back to the VLAN, and disable Network Login on the VLAN (PD3-3599531).

### Proxy ARP Setting Should Take Effect When Network Login is Enabled

When the switch has a proxy ARP setting and Network Login is not enabled, the proxy ARP setting works correctly. However, when you enable Network Login on the port, the actual MAC address is sent back to the ARP request from the switch (PD3-3523432).

### Wireless Clients Forced to Reauthenticate During Roaming

Wireless clients are forced to reauthenticate during roaming under the following conditions:

- When the default-user-vlan is set to wireless Mgmt VLAN
- When the use-dynamic-vlan is set to No in a dot1x configuration

(PD3-3514072)

### Enhanced DOS Protect Rate-Limit Configurations Are Lost

Uploading or downloading configurations does not restore rate limiting for enhanced-dos-protect rate-limit configurations (PD3-3305879).

### Disable Trusted MAC Globally Will Not Automatically Remove Network Login Ports Added as Tagged Port in other VLANs

You cannot disable trusted MAC when a Network Login port is added to a VLAN as a tagged port without first removing the port from the tagged VLAN manually. Running the `disable trusted-mac` command without first manually removing the port from the tagged port generates the following error message:

```
Cannot disable Trusted MAC first remove port 1:4  from Tagged VLAN voice
```

You must remove the Network Login port added as a tagged port in the other VLANs before you disable trusted MAC (PD3-2257721).

### After Network Login Authentication, Cannot Get an iP Address from the DHCP Server

After campus-mode web-based network login is authenticated, the authenticated client cannot get an IP address from the external DHCP server. When network login is removed, you can get a DHCP address from the external DHCP server. This only applies to the Alpine FM32T switch. As a workaround, after you unconfigure the slot on the Alpine FM32T, you can get an IP address from DHCP after authentication (PD2-241015302).

### Wireless Ports Do Not Come Online if VLAN Gets IP Address from BOOTP

If configuring the default VLAN IP from BOOTP, the wireless ports will not come online.

**Workaround.** Manually configure the VLAN IP (PD3-3017425).

### Special Characters Accepted in WEP Plaintext Key

While configuring the WEP Plaintext key, the following characters are accepted in the CLI and are also stored as part of the key:

- - (hyphen)
- _ (underscore)
- . (dot)

For example, eg.con sec open64wep wep key add 0 plaintext a-_.. would be an accepted key.

The following character is accepted in CLI but not stored as part of the key:

- # (hash)

For example, eg.con sec open64wep wep key add 0 plaintext a-_..############ is accepted by the switch, but is seen as identical to the previous example.

The following characters are rejected in the CLI:

- ~‘@$%^&*()+={[}]|\:;"'<,>?/

For example, eg.# con sec open64wep wep key add 0 plaintext abcd' generates a syntax error at the ‘ character.

(PD3-1853431)

### A New ACL Might Not Block Packets

In certain unusual cases, a new ACL might not block packets. If you apply an ACL (without specifying a precedence) to a port, then disable and enable the slot for that port, the ACL functions correctly. However, if you now delete the ACL, then create a new one, it does not block packets (PD2-221267902).

### Roaming Client MAC Might be Aged Out

If a network login client moves from one layer 2 switch to another switch on a different VLAN, the MAC address might be aged out and de-authenticated, generating an error message similar to the following (PD2-191169610):

```
ERROR: Port 1:3 not in vlan
```

### False EAPOL-Flooding Alarm

If both primary and secondary RADIUS servers fail or are unreachable, you might get a false alarm of an EAPOL-Flooding attack in the log. This is most likely to occur after boot-up with large numbers of 802.1x clients (PD2-172518964).

### EAP-Failure Messages Not Sent When Client is Unauthenticated by an Administrator

If an 802.1x supplicant MAC is forced into the unauthenticated state by an administrator, an EAP-Failure message is not sent to the client. Using the `clear netlogin state`, `disable port`, or `restart port` commands can force the client into the unauthenticated state. If this happens, the client is not authenticated, but some 802.1x client applications appear to be authenticated and can cause confusion in troubleshooting. This problem does not occur if the client logs off (PD2-160278605).

### Do Not Upload a Configuration Containing Authenticated Clients

In network login campus mode, do not save and upload a configuration containing authenticated clients. Doing so can corrupt the configuration. To back up a configuration:

1 Disable network login using the `disable netlogin` command.

2 Unauthenticate all client ports using the `clear netlogin state ports vlan` command.

3 Verify that all ports are unauthenticated using the `show netlogin` and `show vlan` commands.

4 Save the configuration using the `save configuration` command.

5 Upload the configuration to your backup server using the `upload configuration` command.

When you download this configuration, remember to enable network login (PD2-142190901).

### The show netlogin Output Might Display Wrong Authentication

If you disable network login, the output of the `show netlogin` command incorrectly displays all existing authenticated 802.1x clients as HTTP. If you enable network login again, the display corrects. This is cosmetic, and does not affect the actual authentication (PD2-171477134).

### ICMP Access Lists and ignore-overlap

The ignore-overlap feature is not supported with ICMP access lists. Use precedence to manage overlapping. If you specify `ignore-overlap` when you create an ICMP access list but do not specify a precedence number, a precedence of 0 is assigned. In addition, the ICMP access list gives the highest precedence to the rules created first, instead of giving precedence to the most specific rule (PD2-157416614).

### CPU DoS Protect and ACL Precedence

If you configure the CPU DoS protect feature with a filter precedence of x, you cannot create an access list with a precedence of x, x+1, or x+2. All other values are acceptable.

If you configure an access list with a precedence of x, you cannot configure the CPU DoS protect feature with a filter precedence of x, x-1 or x-2. All other values are acceptable (PD2-129163428).

### MSM Failover Clears Logins

An MSM failover clears the Network Login state, forcing users to log in again (PD2-109075331).

### Network Login RADIUS Server Interoperability

The following RADIUS authentication servers are tested and supported with Network Login:

- Microsoft Windows 2000 Internet Authentication Service
- Funk Steel-Belted-Radius Enterprise Edition version 4.0

The following authentication methods are supported with Network Login:

- PAP (web-based only)
- EAP-MD5 (802.1x only)
- EAP-TLS (802.1x only)
- EAP-TTLS (802.1x only)
- PEAP (802.1x only)

### Network Login Supplicant Software Interoperability

The following supplicant software applications are tested and supported with Network Login:

- Web-Based: Internet Explorer 6 web browser
- Web-Based: Netscape Navigator 7 web browser
- 802.1x: Microsoft Windows XP native OS client
- 802.1x: Microsoft Windows 2000 Professional native OS client (patch 313664)
- 802.1x: Funk Odyssey Client, version 2.0
- 802.1x: MeetingHouse Data AEGIS Client for Windows, version 2.0.5
- 802.1x: MeetingHouse Data AEGIS for Windows, version 1.3.6.1
- 802.1x: MeetingHouse Data AEGIS for Linux, version 1.1.2

### RADIUS and the BlackDiamond

When RADIUS authentication is configured on a BlackDiamond switch, upon reboot, you will see the following message indicating that the system is initializing before authentication messages will be transmitted to the configured RADIUS server(s) (7046):

```
"Warning: Radius is going to take one minute to initialize."
```

### RADIUS and Telnet

If one of the following two situations occurs:

1. You have a single RADIUS server configured with a RADIUS timeout value of 10 seconds or more
2. Both primary and secondary RADIUS servers lose their connections and the configured RADIUS timeout value is 5 seconds or more

The switch might not be able to fail over to the local user authentication for telnet sessions. If this happens, the switch cannot be accessed via telnet. This does not occur with the default RADIUS timeout configuration of 3 seconds, or when using alternate session types such as console, SSH, or Vista management (PD2-109828821).

### The show netlogin Command Output

If you remove a module with configured Network Login ports and reboot the switch, the output of the `show netlogin` command incorrectly omits the configured ports. Network Login remains enabled on the configured ports and operates correctly if you reinstall the module (PD2-92593101).

## SLB and Flow Redirection

### Do Not Use SLB and NAT on the Same Switch

Do not use SLB and NAT on the same switch (PD2-224957457).

### Enumeration Mode Redirects ICMP Packets

When you create a flow redirection rule for source address based on a subnet mask of /24, enumeration mode is selected, and all ICMP packets are redirected to the next hop. To work around this, use a subnet mask of /16 (PD2-118471863).

### Cache Servers Set To “Down” Under Sustained High Traffic Loads

Under very high sustained loads flow redirection might fail and set a cache server to the “down” state and then bring it back up. This only occurs during high loads for a duration of more than 2 minutes. The server will come back up immediately; however, during that time connections that were established might be dropped due to a flushing of the associated IP forwarding database entries. A “down” state is depicted in the log with the following message:

```
09/01/2000 10:51.56 <INFO:IPRT> redirect next hop test <ip_addr> changed to down
```

### Health Checking Cannot be Disabled

Flow redirection health checking of the next hop address is turned on by default and cannot be disabled.

## NAT

### Do Not Use SLB and NAT on the Same Switch

Do not use SLB and NAT on the same switch (PD2-224957457).

### NAT Rule Configuration Not Updated

If you change the name of a VLAN that is part of your NAT configuration, the NAT rule configuration is not updated. NAT rule matching continues to operate correctly, but if you save or upload the configuration, the rule is saved or uploaded incorrectly (PD2-82963707).

## Vista

### Failed Vista Login Logged Incorrectly

A failed Vista login appears in the syslog with the wrong IP address and login user name (PD2-203782108).

### No 10 Gigabit Option for Port Speed

There is no 10 Gigabit option for the port speed on the port configuration page. To work around this, use the CLI (PD2-208090014).

### SNMP Community and Trapreceiver Information Not Updated

The SNMP community and trapreceiver information is not updated when you refresh the SNMP page (PD2-208635103).

### Use CLI to Configure SNMPv3

You cannot configure SNMPv3 community authentication, information, or trap receivers via Vista. To work around this, use the CLI (PD2-208635101).

### Incorrect Minimum Limit on OSPF Page

The Miscellaneous Parameters on the OSPF page lists a minimum of zero for the costs and timers. The minimum limit is one (PD2-194279901).

### Cannot Create User Accounts

You cannot create a user account using Vista; you can only create admin or pppuser accounts. To work around this, create the account using the CLI (PD2-197374642).

### Cannot Enable STP

You cannot enable a STP domain using Vista. If you try, Vista does not generate an error message, but does not enable STP. (PD2-158471801).

### Alpine 3808 Erroneously Displays Four PSUs

Vista displays PSU C and PSU D on an Alpine 3808 chassis. The Alpine 3808 supports only two PSUs, PSU A and PSU B (PD2-135911601)

### Cannot Add Trap Receiver or Community String

On the SNMP configuration page, if you add a trap receiver or community string Vista indicates success, but does not make the change to the switch. To successfully add a trap receiver or community string, use the CLI (PD2-120713201).

### Blackhole Flag Missing

The blackhole flag is missing from the FDB statistics screen (PD2-129387401).

### Multicast Address Display

If you configure a routing protocol on multiple interfaces, the Vista statistics page displays the wrong Locally Registered Multicast Address (PD2-105094265).

### Configuration Statistics PSU Display

The Vista configuration statistics switch display for the BlackDiamond 6808 shows four power supplies when only two are installed (1-D3RSP).

### Vista and RADIUS

If a switch configured for RADIUS authentication loses communication with the RADIUS server, subsequent attempts to use the Vista Web application will take a very long time (measured in several minutes). When communication is lost with the RADIUS server, Vista will continue to make authentication requests for every page. Each request has a timer that will expire leading to an excessive amount of time to bring up each page (5144).

### Configuration Options with Large Number of Interfaces

When selecting a configuration applet with a large number of configured interfaces, the traversal of the VLAN interfaces by Vista can cause a Watchdog reset due to the task utilization of Vista during the

interface data collection. It is recommended that Vista not be used for configurations with Watchdog enabled where the Vista Configuration applet is used with a large number of VLAN interfaces.

## SNMP

### Extreme Real Time Statistics Does Not Work When There are 24+ Ports

When Network Management tool EPICenter tries to get real time statistics on an Extreme device that has more than 24 ports, it sometimes fails (PD3-15975950).

### Performing an SNMP Mibwalk and Polling qBridgeMIB Might Cause High Utilization

Performing an SNMP mibwalk and polling qBrigeMIB might cause high CPU utilization for the task tSnmpd. You might see error messages similar to the following:

```
08/02/2004 08:36:32.66 <Warn:SYST> task tSnmpd cpu utilization is 81% PC: 80fed744
```

(PD3-3011496).

### ESRP SNMP MIB Table Election Algorithms Missing

The following ESRP election algorithms are not included in the ESRP SNMP MIB table extremeEsrpTable:

- ports-track-priority
- track-ports-priority

The extrmeEsrpNeighborTable should contain the following additional algorithms:

- ports-track-priority-mac
- priority-ports-track-mac
- priority-track-ports-mac
- track-ports-priority-mac
- priority-mac-only
- ports-track-priority
- track-ports-priority

(PD2-244686415)

### The configure snmp community Command Replaced

The `configure snmp community` command has been replaced by the `configure snmp add community` command. Though you can enter the `configure snmp community` command, it has no effect (PD2-225385999).

### Only Warm Start Smart Trap Sent After Power Cycle

When a switch is power cycled, only a warm start smart trap is sent. Previously, a cold start smart trap was sent (PD2-209311102).

### extremeVlanGlobalMappingTable Exists only for Backward Compatibility

The extremeVlanGlobalMappingTable exists only for backward compatibility and has no specific value (PD2-204237301).

### ExtremeEapsTable Not Browsable

The ExtremeEapsTable is not browsable. It is used only for SNMP traps (PD2-176373732).

### MIB Does Not Differentiate Between 110 and 220 VAC

The Inputpower MIB attribute does not differentiate between 110 VAC and 220 VAC PSUs in BlackDiamond 6804, BlackDiamond 6816, Alpine, or Summit switches (PD2-199834514).

### The trapDestOwner is Required in the trapDestTable

ExtremeWare 7.1 (and later) requires the trapDestOwner in the trapDestTable to send the community, address, owner, and status in the create request for the trapreceiver entry through SNMP (PD2-126200001).

### Cannot Delete Default Community Strings

You cannot delete the default community strings (*public* and *private*) using the `configure snmpv3 delete community` command. To delete these strings, use the `configure snmp delete community` command (PD2-153687501).

### Do Not Configure an SNMPv3 Community String with more than 32 Characters

You cannot configure an SNMPv3 community string with more than 32 characters. If you download a configuration containing such a string, that line in the configuration fails, returning the following error message to the console (PD2-150132207):

```
ERROR : SNMPV3 Community Creation Failed
```

The rest of the configuration loads correctly.

### Modular Switch get Error

A get request from an NMS to a modular switch for the ifMau<object> on the management port returns a “no such instance” error (PD2-124250702).

### SNMP and ACLs

Polling the ACL table with a network manager can cause high CPU utilization. For example, with 1,000 ACLs, CPU utilization could be as high as 95%, which could make the console unresponsive (PD2-57475201).

### Incrementing the Interface Value

With a getnext or bulkget on a non-existent ifIndex of an object ID, the agent returns next OID value instead of incrementing the ifIndex (2-H1OOF, 2-GZ52P).

### Trap Receivers as Broadcast Entry

Although it is possible to enter a broadcast or IP multicast address as an SNMP trap receiver, it will not function (2545).

### Bridge MIB Attributes

The IEEE Bridge MIB dot1dTpPortEntry PortInDiscards and dot1dBasePortEntry counters do not increment (4937).

### SNMP Time-out Setting

SNMP management stations might need to set the SNMP time-out value to 10 seconds as some large configuration operations take longer to perform (7151).

In addition, when using SNMP tools that use the bulk get request function as opposed to generic get next requests, the MIB walk can time out and subsequently fail with the default time-out setting. It is suggested that the default time-out value be increased from 5 seconds to 60 seconds to decrease the frequency of such time-outs when the get bulk request contains a large number of entries (9592).

### SNMP Access Profile

The access profile for SNMP read-only or SNMP read-write can be used for permit-mode only, deny-mode is not operational (7153).

### SNMP and Auto-negotiation Settings

For 100/1000Base-TX ports, the ifMauAutoNegAdminStatus can only be disabled if the ifMauDefaultType is set to a speed of 100 Mbps. For 10/100Base-TX ports, you must first set the value of ifMauDefaultType to the correct setting before disabling the ifMauAutoNegAdminStatus (9416).

### SNMP and the FDB MIB

When exercising the route table in the FDB MIB with dot1dTpFdbTable enabled, high CPU utilization messages might be displayed in the syslog. This occurs when there is a large number of FDB entries and has no adverse affects on protocol stability (PD2-102926801).

### Extreme Fan Traps

The `extremeFanOK` and `extremeFanFailed` traps will contain the `extremeFanNumber` indicating which fan has failed (1-7J571).

### Extreme Power Supply Traps

A new object was added “extremePowerSupplyNumber” to the power supply traps. The two RPS traps will no longer be sent out. Instead the extremePowerSupplyGood and extremePowerSupplyFail traps will contain the power supply number indicating which power supply has failed (1-7J56T).

# Diagnostics and Troubleshooting

## FDB-Scan Does Not Upgrade Properly

If you are upgrading a switch using an ExtremeWare 6.2.2 or later based image, for example, ExtremeWare 6.2.2b156, by default, `fdb-scan` is set to `disabled` and the `failure-action` is set to `log` only. When you save the configuration and upload with image ExtremeWare 7.1.1b16 or ExtremeWare 7.2.0b25, the fdb-scan configuration changes to `fdb-scan enabled`, and `failure action sys-health-check` (PD2-245655236).

## OC12 Module Might Report False External Loopback Failure on External Test

When running normal or extended diagnostics on an OC12 module, the switch might incorrectly report that the specified port fails when performing the external loopback diagnostic test (PD3-796908).

## A3ci Running Normal Diagnostics Hangs in the "diag" State

Repeatedly running normal diagnostics on an A3ci hangs the switch in the `diag` state. For example, running normal diagnostics on a module might generate the following error message on the console:

```
Double free or memory being overwritten.
sbmfree double (0/10629/1/0x84d9daf0/0x84d9db00)
```

(PD2-249307801)

## NP Module Error Messages in the Log After Running Diagnostics

NP heartbeat and reboot error messages are shown in the log when running extended diagnostics on NP based modules. The same error messages are also shown on the OC3 and ATM modules (PD2-237117101).

## Errors Not Displayed in show diagnostics Output

If you run extended diagnostics, diagnosed errors are recorded in the log, but are not shown in the output of the `show diagnostics` command (PD2-225483201).

## Incorrect show diagnostics Output for BlackDiamond 6816

The output of the `show diagnostics` command displays BlackDiamond 6816 slots A, B, C, and D as 17, 18, 19, and 20 (PD2-106752601).

## Entering q Does Not Quit Diagnostics Display

Entering `q` to quit the `show diagnostics sys-health-check` display does not quit the display (PD2-145117543).

## Single MSM Not Taken Offline

If you have only one MSM installed in a BlackDiamond chassis, you configure the system health check alarm level to `card-down`, and eight errors are detected, the MSM is not taken offline. The MSM remains fully operational (PD2-143167301).

### Automatic Memory Scanning Can Trigger Incorrect Reboot Loop Detection

On Summit and Alpine switches, if memory scanning is automatically initiated via the `auto-recovery` parameter in the `configure sys-health-check` command and the reboot loop detection threshold is 1, the system might incorrectly detect a reboot loop and come up in minimal mode (PD2-140185601).

### Packet Diagnostics Display Backplane Incorrectly

When you run packet diagnostics on the Alpine 3804, the console displays the backplane as slot 5. The display is wrong: the diagnostics are correctly running on the backplane. The extended diagnostics console display is correct (PD2-151752701).

### Packet Diagnostics Display Wrong Slot Name

When you run packet diagnostics on the MSM in slot B, the console displays the slot as slot 10, instead of MSM-B. The display is wrong: the diagnostics are correctly running on the MSM in slot B. The extended diagnostics console display is correct (PD2-138607801).

### Bus-Stats Error Messages

The `show config detail` command output displays the following new commands:

```
disable bus-stats
configure bus-stats window history 3
configure bus-stats window errors 3
configure bus-stats threshold slow-path x
configure bus-stats threshold fast-path y
```

The bus-stats feature helps filter erroneous log messages related to transient hardware errors. It is disabled by default and should only be enabled when troubleshooting transient hardware errors. Enabling this feature requires activation by Extreme Networks personnel.

### Spurious Message When system-down is Configured

If you configure the system health check alarm level for system-down and a fault is detected, the switch is turned off but continuously logs the message “Card in slot N is off line.” You can ignore this message (PD2-129386201).

### The use configuration Command

When the switch is in minimum mode, the `use configuration` command has no effect on the backup MSM (PD2-129133801).

### Output of the show diagnostics Command

The output of the `show diagnostics` command for the CPU system might display negative numbers, and the totals might not add up properly (PD2-128460401).

### Configure Auto-Recovery to online or Alarm-Level to traps

If you configure the system health check auto-recovery to `offline`, save the configuration, and configure the alarm-level to `log`, a health check brings the module or switch offline regardless of how many errors the health check detects. To avoid this, either configure auto-recovery to `online`, or configure alarm-level to `traps` (PD2-124368101).

### Error Count Not Accurate

If the switch is flooded with heavy traffic for more than 10 minutes, the `CPU System` field in the `show diagnostics` output is not accurate. The display reports up to 20 more errors (PD2-122738701).

### Configuring Diagnostics Mode Off

If you configure diagnostics mode OFF, and then execute the `unconfigure switch all` command, when the switch returns to the active state the diagnostics mode is still set to OFF. The default diagnostics mode should be `fastpost`. To verify which diagnostics mode is set for the switch, use the `show switch` command (1-97NL1).

### Disable Remote Syslog Before Enabling IPARP Debug-Tracing

With remote syslog enabled, if you configure the IPARP debug-trace to level 2 or higher, the switch hangs and is rebooted by the watchdog timer. To avoid this, disable the remote syslog prior to configuring the debug-trace (PD2-110983505).

## Bridging

### Extended Diagnostics Does Not Include Backplane Connection

After running extended diagnostics on a slot, the mirror ptag will not include the backplane connection (PD3-2016265).

## Documentation

### enable rip originate-default Command Description is Incorrect

The description for the `enable rip originate-default` command in the *ExtremeWare Software Command Reference G*uide, *Software Version 7.3.0* should read:

If `always` is specified, RIP always advertises the default route to its neighbors. If `always` is not specified, RIP adds a default route if a reachable default route is in the route table.

(PD3-19630241)

### VRRP and ESRP Can Be Simultaneously Enabled

After ExtremeWare 6.2.1, VRRP and ESRP can be simultaneously enabled on the same switch. On page 352 of the *ExtremeWare Software User Guide, Software Release 7.1.0*, the second bulleted item at the top of the page states that "VRRP and ESRP cannot be simultaneously enabled on the same switch," which is incorrect (PD2-233846470, PD2-233846479).

### Summit48si LED Description Incorrect

The LED activity listed in Table 29 on page 85 of the *Extreme Networks Consolidated "i" Series Hardware Installation Guide* is not correct. The Summit48si does not support 100/1000 Mbps Speed LEDs and 10/100 management port LEDs. Mini-GBIC port status LED information needs to be added to the table (PD3-3523168).

### reauth-period Range is Not Correct

The `reauth-period` range is not correct in the *ExtremeWare 7.3 Software User Guide*. The correct range is 600-60000 seconds (PD3-3455541, PD3-3455681).

### EAPS is now supported with Basic Layer 3 License

With ExtremeWare 7.3, EAPS is now fully supported with the Basic Layer 3 license. However, this ExtremeWare 7.3 licensing change is not included in the Software Licensing section of the *ExtremeWare 7.3 Software User Guide*. This change will be included in the next version of the *ExtremeWare 7.3 Software User Guide*.

### The Auto-Recovery Threshold Applies only to BlackDiamond I/O Modules

The auto-recovery threshold in the `configure sys-health-check` command applies only to BlackDiamond I/O modules.

### Configure Auto Negotiation to Recognize Single Fiber Failure as Port Failure

If you want the switch to recognize a single fiber failure as a port failure, configure autonegotiation on both ends of the link (PD2-210751796).

## UAA

### TCP Transmission Causes an SNMP Send Error when the AP Comes Up

TCP transmission causes an SNMP send error when the AP comes up and generates the following error message:

```
SYST: Port 1:20 link active 100Mbs FULL duplex
WLANSYS: <WLAN> Port 1:20 Wireless Port Down
WLANSYS: <WLAN> Port 1:20 SNMP tcp send : subagent send failed
SYST: Port 1:20 link down
SYST: Port 1:20 link active 100Mbs FULL duplex
SYST: Port 1:20 link down
SYST: Port 1:20 link active 100Mbs FULL duplex
WLANSYS: <WLAN> Port 1:20 Wireless Port Up
```

This error message is harmless and can be safely ignored (PD3-7035411).

### Some IAPP Debug Messages Are Not Logged

If you configure debug-trace for wireless ports to debug-level 5 and set the syslogd priority to debug, when you roam from one AP to another AP, the `show log` command does not display all of the IAPP debug messages, whereas the `show wireless ports x:y log` command displays all IAPP debug messages correctly (PD3-7040404).

### DHCP Port is Disabled When Changing a VLAN Tag

DHCP ports are disabled if you change the VLAN tag to a new value when configuring the DHCP address range for the specified VLAN. Use caution when changing VLAN tags (PD3-9243378).

### Port Related Configuration Returns an Error During Configuration Download

Downloading a new configuration causes all port related commands to return the error:

```
Port X on card Y is out of range
```

This error occurs when line cards are not configured in the slots (PD3-9259162).

### ifSpecific Variable of ifEntry Table Shows Incorrect Characters for Wireless Interfaces

When retrieving values for the ifEntry table from the SNMP Manager, the ifSpecific variables show incorrect characters for the wireless interfaces (PD3-9511695).

# Issues Resolved in ExtremeWare 7.3.2b3

The following issues were resolved in ExtremeWare 7.3.2.b3Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.3 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, and ExtremeWare 7.2.0b33. For information on those fixes, see the release notes for those releases.

## General

Using smart redundancy on a Summit 48si switch with ports 49 and 50 set in Software Redundant Port (SRP) no longer causes link flapping on the neighboring switches (PD3-14292583).

tSlowTimer task no longer has high utilization in polling for GBIC insertion/removal status that is required for the Smart Trap feature (PD3-24938366).

Unexpected phantom disconnects are no longer occurring on Alpine switches (PD3-24392711).

A trap is no longer sent from the AP to the Summit 300 switch during Network Login, allowing memory to be allocated correctly (PD3-23979971).

During the above, Console or telnet did not hung. We are suspecting could be possible once all memory been leaked.

The switch no longer prints `tNetTask: (ptagDel) Otp index fff in restricted range` messages after an IGMP snooping entry times out (PD3-23319673).

The source IP address for syslog is set properly after rebooting the switch (PD3-23076125).

IP broadcast traffic is now forwarded through the primary subnet in a multinet configuration (PD3-23075999).

IPX/RIP and IPX/SAP updates are now advertised from the ESRP domain master switch so you no longer have to configure a separate ESRP instance for an IPX VLAN (PD3-13366466).

In software redundant gigabit ports on a Summit 48si, the link state is now correctly changed when removing and reinserting redundant links with the master link in the inactive state (PD3-23070976, PD3-18120486, PD3-16714633, PD3-3891361).

When you insert G8xi blades into slots 1, 2, and 4 of a BlackDiamond 6804 chassis and then connect two 1-gigabit Ethernet ports from the BlackDiamond chassis to a Summit 400 port 49 and 50, the link now comes up (PD3-18567133, PD3-18487496).

## BlackDiamond

After upgrading a BlackDiamond and rebooting the switch, the connection recovered message is logged if the backplane connection is restored (PD3-23076376, PD3-14385950)

## Summit

The interframe gap for 100 Mbps ports is now 0.96 micro seconds; the interframe gap for 1 gigabit ports is 0.096 micro seconds (PD3-24639595).

## Spanning Tree Protocol

The STP timer delay no longer exceeds system capacity resulting in an error message (PD3-24882757).

## Bridging

Broadcast and multicast packets are no longer forwarded back to the same port on the EAPS master node after disabling a slot (PD3-23075108, PD3-20010669).

The mirror ptag now includes the backplane connection after running extended diagnostics on a slot (PD3-2016265, PD3-2016224).

## Diagnostics

ExtremeWare diagnostics for V1 modules are not supported beginning with ExtremeWare 7.3.2 (PD3-17352311).

Extended diagnostics results are now properly displayed under the output of the `show diagnostics` command in a Summit 5i (PD3-23075818, PD3-7716811).

## EAPS

The `show msm-failover` command no longer shows a status of "not available" after disabling a port in an EAPS ring, and the error LED no longer lights on the secondary MSM (PD3-23070849, PD3-20894085).

## Mirroring

When a port is added in a mirroring configuration, the packets egressing that port are now mirrored (PD3-22589641).

## RADIUS

When configuring RADIUS Accounting authentication, the Acct-Delay-Time attribute is now set to 6 octets (PD3-14621151, PD2-121179519).

## Routing

Output for the `show configuration` command no longer lists `disable pim-snooping` twice (PD3-23076249, PD3-15128548).

You can send PIM bootstrap packets with a length of more than 1700 bytes without causing the system to fail (PD3-22561358, PD3-22561301).

(S,G) lookup is only performed on PIM neighbor interfaces (PD3-23070721, PD2-209013501).

### SNMP

When a tagged port is deleted from a VLAN using SNMP, the same port is no longer added as an untagged port to the same VLAN (PD3-23075235, PD3-20877560).

# Issues Resolved in ExtremeWare 7.3.1b3

The following issues were resolved in ExtremeWare 7.3.1b3. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.3 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, and ExtremeWare 7.2.0b33. For information on those fixes, see the release notes for those releases.

## General

In software redundant gigabyte ports on a Summit 48si, the link state is now correctly changed when removing and reinserting redundant links with the master link in the inactive state (PD3-16714633, PD3-3891361).

The announce packet counter is now reset:

- When the AP comes online after booting up (PD3-11205415, PD3-11063925).
- When the `reset wireless ports` command is issued (PD3-11205198, PD3-11063647).

## EAPS

Traffic rates no longer drop through a rate shaped port when a link goes down in an EAPS ring (PD3-10676565, PD3-10325999).

## Multicast

Multicast forwarding does not stop when the primary CMT port comes back online (PD3-16694957, PD3-14695885).

Multicast packets are no longer forwarded on all CMT ports when IGMP snooping is enabled and a static IGMP group is configured on the CMT port (PD3-16716924, PD3-14709876).

## Network Login

In Campus mode wireless Network Login, when a *temp* VLAN FDB entry ages out, the Network Login user is not logged out (PD3-16131121, PD3-15254063).

## Security and Access Policies

When performing dot1x authentication in Campus mode with WinXP as the supplicant (EAP-MD5 authentication) and the IAS server as the authentication server, if you stop the RADIUS server, the port no longer tries to authenticate when the ReAuth-Timer expires (PD3-2113971).

## SNMP

All VLAN IP addresses are now shown in the walk results for SNMPwalk (PD3-5101141, PD3-5089821).

The entPhysicalDescr field no longer shows the "NP P3ci" module as "I/O Module" in the entity MIB (PD3-16714281, PD3-3363432).

## VLANs

With 100+ IP VLANs, control packets such as VRRP, are now processed in a timely manner, no longer causing VRRP to flip (PD3-16694591, PD3-1601045).

# Issues Resolved in ExtremeWare 7.3.0b49

The following issues were resolved in ExtremeWare 7.3.0b49. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.3 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, and ExtremeWare 7.2.0b33. For information on those fixes, see the release notes for those releases.

## General

If you repeatedly issue the `show pim snooping <vlan>` command, you no longer get an error message indicating a task failure (PD3-3130511).

If you use the `wireless` command to attempt to configure an IP address on a port that is not capable of wireless transmission, you now receive the message that the port is not capable of wireless transmission (PD3-2809871).

When you change the country code on a switch that does not allow 802.11g operation, the software now forces radio mode to “b” and will no longer accept RF profiles with radio mode = g or bg after the country code has been changed (PD3-3868563).

The error message “no data in retrieved...” no longer appears in the switch log after issuing the `show wireless ap-scan results` command (PD3-2437917).

If you upload a configuration that contains `configure wireless default-gateway 0.0.0.0,` the system now uploads the IP address correctly when uploading the configuration (PD3-3017593).

You no longer get an error message stating that buffer corruption was detected when you attempt to change the value of the management VLAN tag on the wireless equipment (PD3-2997010).

## Alpine

The wrong time stamp is no longer displayed for off channel scanning when the timestamp of the switch is changed (PD3-2634620).

## Security and Access Policies

SSH sessions now end gracefully when you use PuTTY as the SSH client to access the switch and close the PuTTY window without first logging out (PD3-3039712).

After issuing the `clear netlogin state port x` command, there is no longer an authentication delay when PEAP Authentication is used between the supplicant and the authentication server (PD3-3099978).

When using Sygate and Network Login, you can now move a port to another VLAN once it is authenticated (PD3-3004471).

If you change a user password on an 802.1x authenticated session the session no longer becomes unauthenticated (PD3-3149563).

A range check is no longer needed to avoid system failures during snmpsetv (PD3-3455551).

You can now configure SSL HTTPS is enabled (PD3-2956151).

The `show security-profile unsecure` command no longer displays ports that are not capable of wireless transmission and no longer displays interface 2 twice in the command output (PD3-3429031, PD3-3197291).

## UAA

Off channel AP scan now runs when the ALL channel option is selected (PD3-3839591).

## QoS

Ingress QoS configurations are no longer accepted for non-Triumph ports (PD2-241056358).

## PoE

The switch no longer downloads firmware when a firmware download is not required (PD3-2666565).

## SNMP

When you configure a WEP client login and an 802.1x client login, a Network Login trap is now sent to the switch (PD3-2707447).

## ESRP

After you enable ESRP on a VLAN with an IP address and no active ports, and disable ESRP on that VLAN, the route now becomes active (PD2-222505901, PD2-247722501).

## CLI

When you create a VLAN (for example, v1), add a jumbo port, and assign an IP address to the VLAN, the switch now prompts you with "`WARNING: Set MTU for v1 to support jumbo frames or IP fragmentation with jumbo frames`." To do this, use the `configure ip-mtu <number>` command (PD2-241047417).

The watchdog no longer expires when generating an SSL certificate with a 4096-bit key (PD3-2944771).

The switch now automatically disables Web HTTPS after downloading a new certificate or private key and enabling Web HTTPS (PD2-233940698).

# Issues Resolved in ExtremeWare 7.3.0b44

The following issues were resolved in ExtremeWare 7.3. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.3 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, and ExtremeWare 7.2.0b33. For information on those fixes, see the release notes for those releases.

## General

Issuing the `enable system-watchdog` and `enable rmon` commands no longer results in a tRootTask EPC when the watchdog timer is set to enabled (PD2-229063553, PD2-249686302)

LACP is now supported on ExtremeWare 7.3.

When configuring a large number of VLANs, or rebooting a switch with a large number of VLANs, the SNMP management agent will be unavailable for several minutes (PD3-2530177).

The TCP/IP stack no longer answers ICMP mask request queries by default (PD2-181133146).

The syslog no longer fills with messages that state “Session idle timeout” (PD2-219911435).

The ACLs now work properly when you disable and enable an I/O module, and then delete and add the same ACL (PD2-218852668, PD2-249671154).

A session idle timeout message is no longer logged every time you log out of a telnet or console session (PD2-222159327, PD2-249685239).

When you configure a DHCP address range on a VLAN for netlogin, and disable IGMP snooping on the VLAN, the host PC can now allocate the IP address correctly (PD2-223297632, PD2-249685264).

Redundant ports no longer flap after one failover when smart redundancy has been disabled using the `disable smart redundancy` command (PD2-225473428, PD2-249685290).

## Summit

If you use Vista to add a port to a VLAN and delete that port, the port is no longer added to the VLAN every time you add a port using Vista (PD2-212786084, PD2-227975796).

## BlackDiamond

SR XENPAK now works on a BlackDiamond (PD2-236755811).

With BootROM 8.1, using the `reboot slot [msm-a | msm-b]` command via a direct console connection to a slave MSM no longer locks up the MSM. (PD2-225327825, PD2-225764302).

An invalid IP address can no longer be configured when creating a new RSVP-TE path. Use the `show mpls rsvp-te path` command to verify the end point IP address (PD2-162547301, PD2-229594001).

When you configure an RSVP-TE LSP and enable MPLS, traffic can now be transmitted over the RSVP-TE LSPs and TLS tunnels can be established (PD2-249671130).

You can now configure an RSVP-TE LSP and enable MPLS. RSVP-TE: LSPs cannot be established. No traffic can flow over RSVP-TE LSPs and TLS tunnels cannot be established (PD2-249671130).

If you specify a VLAN as the local end point for an RSVP-TE path, the switch no longer allows you to change the VLAN's IP address, unconfigure the IP address, or delete the VLAN. Use the `show mpls rsvp-te path` command to verify the local end point configuration (PD2-164224901, PD2-229594005).

Removing the MSM in a BlackDiamond switch doing MPLS TLS no longer causes some of the FDB entries to start aging (PD2-199171614).

## Alpine

When you reseat the fan tray in an Alpine 3804 or Alpine 3808, the status LED on the SMMi blinks (PD2-205947223).

## Vista

If you configure a new VLAN tag the same as an existing loopback VID, the httpd task no longer crashes (PD2-187697373).

## SNMP

When using SNMP to configure an MSM-3, the SNMPv3 configuration is now preserved after an MSM failover (PD2-170807501, PD2-230083730).

SNMPv3 configuration now includes an encrypted keyword so that there are no longer any increment download failures. You can also now manually cut or paste the configuration to another switch without causing a system failure (PD2-227273841, PD2-249685296).

## Spanning Tree

The `vlan` keyword can now be used with the `enable/disable stpd ports <portlist>` command (PD3-1362824).

## Security and Access Policies

If an FDB rule has the `ignore-overlap` option set, similar IP ACL rules can now be created (PD2-197365033, PD2-227975790).

The following RADIUS demultiplexer handler error message has been changed from Warning to Informational:

```
<INFO:WLAN> <WLAN> Port 1:44 Radius server 1 no handler for demux id 168
```

(PD2-237095201)

## Switching and VLANs

Using the `show vlan stats` command on multiple VLANs no longer stops switch-bound ping and Telnet packets. The Summit48si no longer drops Layer 2 packets (PD2-225385621, PD2-249685284).

## Network Login

When you enable Network Login on a port, the switch now behaves as a full DHCP server, sending all DHCP NAK packets to the port when you enable DHCP (PD2-195081355, PD2-249660679).

The order in which you configure web-based Network Login settings no longer causes configuration errors when parsing downloaded configurations (PD2-160278607, PD2-180726753).

## Diagnostics

Extended diagnostics no longer fail on T1 I/O modules on the Alpine switch causing the chassis to go into limited commands mode (PD2-227975774).

## VRRP

The VRRP MAC index table now initializes properly after an I/O reset (PD2-249660650).

## BlackDiamond

ExtremeWare can now access the EEPROM of the slave MSM and I/O modules (PD3-19662516).